高职高专网络技术专业岗位能力构建系列教程

网络安全部署

郭 琳 编著

清华大学出版社

高职高专网络技术专业岗位能力构建系列教程

网络安全部署

郭　琳　编著

清华大学出版社
北　京

内 容 简 介

本书着眼于网络安全工程师岗位需求，结合网络安全部署和发展现状，以防范企业网常见网络攻击为目标，以企业网络常见安全防护技术为主导，以配置与管理企业网络安全设备为主线，以 3 个学习情境为流程，循序渐进地讲解了相应的网络安全工作任务。本书以任务驱动组织内容，3 个学习情境共设计了 16 个工作任务，并在每个工作任务后面都安排了满足职业资格考证的过关练习。本书的编写以提高学生应用能力为宗旨，按照企业对高校学生的实际需求来设计学习情境和工作任务，使学生能够在了解相关理论的基础上，具备相应的实际操作技能。

本书可作为高职高专计算机网络和信息安全专业教学用书，也可作为大中专院校、计算机培训班的实训指导教材，还可作为网络安全技术人员、网络安全爱好者、网络管理人员和信息安全管理人员的参考书。

图书在版编目(CIP)数据

网络安全部署/郭琳编著. —北京：清华大学出版社，2012.11
（高职高专网络技术专业岗位能力构建系列教程）
ISBN 978-7-302-29019-3

Ⅰ. ①网… Ⅱ. ①郭… Ⅲ. ①计算机网络－安全技术－高等职业教育－教育 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 124391 号

责任编辑：刘 青
封面设计：傅瑞学
责任校对：袁 芳
责任印制：

出版发行：清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座　　**邮 编**：100084
社 总 机：010-62770175　　**邮 购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795764
印 刷 者：
装 订 者：
经 销：全国新华书店
开 本：185mm×260mm　　**印 张**：19.25　　**字 数**：457 千字
版 次：2012 年 11 月第 1 版　　**印 次**：2012 年 11 月第1 次印刷
印 数：1～ 000
定 价： .00 元

产品编号：038817-01

高职高专网络技术专业岗位能力构建系列教程

出版说明

信息技术是当今世界社会经济发展的重要驱动力，网络技术对信息社会发展的重要性更是不言而喻。随着互联网技术的普及和推广，人们日常学习和工作越来越依赖于网络。目前，各行各业都处在全面网络化和信息化建设进程中，对网络技能型人才的需求也与日俱增，计算机网络行业已成为技术人才稀缺的行业之一。为了培养适应现代信息技术发展的网络技能型人才，高职高专院校网络技术及相关专业的课程建设与改革就显得尤为重要。

近年来，众多高职高专院校对人才培养模式、专业建设、课程建设、师资建设、实训基地建设等进行了大量的改革与探索，以适应社会对高技能人才的培养要求。在网络专业建设中，从网络工程、网络管理岗位需求出发进行课程规划和建设，是网络技能型人才培养的必由之路。基于此，我们组织高校教育教学专家、专业负责人、骨干教师、企业管理人员和工程技术人员对相应的职业岗位进行调研、剖析，并成立教材编写委员会，对课程体系进行重新规划，编写本系列教程。

本系列教程的编写委员会成员由从事高职高专教育的专家，高职院校主管教学的院长、系主任、教研室主任等组成，主要编撰者都是院校网络专业负责人或相应企业的资深工程师。

本系列教程采用项目导向、任务驱动的教学方法，以培养学生的岗位能力为着眼点，面向岗位设计教学项目，融教、学、做为一体，力争做到学得会、用得上。在讲授专业技能和知识的同时，也注重学生职业素养、科学思维方式与创新能力的培养，并体现新技术、新工艺、新标准。本系列教程对应的岗位能力包括计算机及网络设备营销能力、计算机设备的组装与维护能力、网页设计能力、综合布线设计与施工能力、网络工程实施能力、网站策划与开发能力、网络安全管理能力及网络系统集成能力等。

为了满足教师教学的需要，我们免费提供教学课件、习题解答、素材库等，以及其他辅助教学的资料。

后续，我们会密切关注网络技术和教学的发展趋势，以及社会就业岗位的新需求和变化，及时对系列教程进行完善和补充，吸纳新模式、适用的课程教材。同时，非常欢迎专家、教师对本系列教程提出宝贵意见，也非常欢迎专家、教师积极参与我们的教材建设，群策群力，为我国高等职业教育提供优秀的、有鲜明特色的教材。

高职高专网络技术专业岗位能力构建系列教程编写委员会

清华大学出版社

2011年4月



近几年来，随着网络应用的飞速发展，企业网中各种网络攻击事件层出不穷，对网络管理员和网络安全工作者提出了更高的要求。教育部[2006]16号文明确指出课程建设与改革是提高教学质量的核心，也是教学改革的重点和难点。高等职业院校要积极与行业企业合作开发课程，根据技术领域和职业岗位（群）的任职要求，参照相关的职业资格标准，改革课程体系和教学内容。本书从实际出发，以工作任务的形式介绍企业网中常见的网络攻击行为和防御手段，以及企业网络硬件的配置和管理方法。

1. 课程的编写原则

教材以“工学结合”为理念，精选企业网中网络所受到的威胁，以及进行安全防护、管理的完整工作过程，按照公司的拓扑和业务需求做出规划，并根据课程的内容和特点设计各种典型应用的工作任务，做到学习过程和工作过程的高度一致。每个任务的学习过程以工作过程为导向，最终形成学生的职业能力，缩短学生理论学习与实际应用之间的距离。教材选编和规划的知识具有专业化、体系化、全面化特征，能体现和代表当前最新的网络技术发展方向。将市场所需的网络技能融进若干案例中进行讲解，充分体现项目案例驱动的课程设计思想。

2. 课程的内容设计

教材共设计了3个学习情境，每个学习情境对应企业网络中不同的安全需求。学习情境一：企业网中常见网络攻击分析；学习情境二：企业网中常见防护技术分析；学习情境三：企业网中主要网络设备的安全配置。每个学习情境中都设计了若干个工作任务，每个工作任务为具体的企业需求提出解决方案和措施。每个工作任务的编写以“用户需求与分析→预备知识→方案设计→任务实施→常见问题解答→过关练习”的形式组织，深入浅出地培养学生的职业技能。教材表达精练、准确、科学，图文并茂，以提高学生的学习兴趣。教材的编写中注重对学生学习方法的指导，体现知识的联想发展，促进学生自主探索、温故知新。教材中的活动设计以学生为本，以培养学生的职业能力和素质为目标，内容具体，并具有可操作性。

3. 课程的实施环境和教学方法

教材中所设计的工作任务绝大多数都可以借助虚拟机、模拟器等软件在一台配置较高的计算机上完成，使学生可以在课外单机环境下随时完成本书所设计的知识与技能的学习。在实训室的课内教学则至少每2人配备1台计算机。每组工作台包括一台交换机、一台防火墙、一台VPN、一台IDS和若干根网线。工作任务分小组完成。每组6～8名同学，选择

一名组长承担管理工作，负责任务分派和工作安排。课程教师可以根据需要随时调整任务内容，负责技术咨询和指导工作，控制任务的实施。

4. 课程职业认证

校企合作的重要意义在于把企业对人才的技能需求直接传递到课堂教学中，缩短人才的培养时间，提高人才的培养效率。学生在全部学习完本课程后，可以根据所掌握专业知识的深浅程度，有针对性地参加国家软考网络工程师或网络管理员的考试，以证明个人的职业能力，加强就业的竞争力。

5. 学习和交流

为了便于网络安全课程教师之间、教师与行业企业专家之间进行信息安全方面的经验交流，我们建立了“信息安全技术”QQ群，群号是50235190。本教材编者的邮箱是guolin416@126.com。通过这些方式可以实现广泛交流，以及在本教材中所涉及的课件、文档和视频等资源的共享。我们正在建设本教材对应的课程网站，教材所涉及的资源将逐步上网以方便互相学习和交流使用。

6. 合作和致谢

全书由郭琳编著。在本书的编写过程中，得到了蓝盾信息安全技术股份有限公司、星网锐捷网络有限公司、深圳职业技术学院、长春职业技术学院、襄樊职业技术学院、北京信息职业技术学院等企事业单位和兄弟院校的大力支持，在这里一并表示衷心的感谢。另外，向朱义勇老师、张宇辉老师、杨斌老师、钟名春老师、陈明老师、石淑华老师对本书出版做出的特殊贡献深表谢意。

由于编者水平有限，错漏之处在所难免，敬请同行专家和读者给予批评指正。

编　者

2012年5月







学习情境一　企业网中常见网络攻击分析

学习情境二 企业网中常见防护技术分析

学习情境一

企业网中常见网络攻击分析

随着互联网的飞速发展，网络的安全问题显得日益重要。每一台与互联网连接的计算机都有可能成为黑客的攻击对象。那些防范意识较差或者对网络安全不甚了解的用户，都极易成为黑客攻击的目标。当计算机用户上网聊天、浏览网页、下载文件时，无论是登录账号、密码，还是电子邮件，甚至涉及商业秘密的文档操作都有可能被黑客偷窥。学习情境一主要对黑客的定义、历史，常用的攻击工具及手段做了详尽的叙述，以实际的案例，带领大家进入黑客的世界，以实例的方式让读者了解黑客的攻击手法，从而采取各种防护策略，让黑客无从下手，让系统更为安全。

黑客技术就像一把双刃剑，它可以入侵他人的计算机，但是也可以通过了解黑客入侵的手段，知道如何防护自己的计算机，以保护计算机不受他人的入侵。通过本学习情境所有工作任务的实践，揭秘黑客攻击的手法，盘点常见的黑客命令、端口扫描与入侵、局域网嗅探、远程控制、拒绝服务攻击等当前比较流行的黑客入侵技术，让大家对常见的网络攻击手段了如指掌，以使用攻防互渗的防御方法，全面确保用户的网络安全。

本学习情境需要完成的工作任务如下：

工作任务一　了解常见黑客命令
工作任务二　目标系统的探测
工作任务三　口令破解
工作任务四　网络监听工具的使用
工作任务五　远程控制
工作任务六　拒绝服务攻击

工作任务一

了解常见黑客命令

1.1 用户需求与分析

提起网络安全问题，人们便不由自主地联想到黑客，将他们和破坏网络安全、盗取网络账户等问题联系起来。由于少数高水平的黑客可以随意入侵他人的计算机，并在被攻击者毫不知晓的情况下窃取计算机中的信息后悄悄退出，于是人们对此产生了较强的好奇心和学习黑客技术的欲望，并在了解黑客攻击技术之后不计后果地进行尝试，给网络带来了极大的威胁。黑客进行攻击的常见理由有：想在他人面前炫耀自己的技术，让他人更崇拜自己；看不惯某人、某单位的某些做法，攻击他们的计算机给他们一种教训；纯粹为了好玩、恶作剧；练习，为了成为一名高手做实验；窃取数据，谋取经济利益。其实黑客及黑客技术并不神秘，也不高深。一个普通的网民在具备了一定的基础知识后，也可以成为一名黑客。黑客技术是一把双刃剑，通过它既可以入侵他人的计算机，又可以了解黑客的入侵手段，掌握保护计算机、防范入侵的方法。在学习黑客技术时，应该首先明确学习的正确目的。

黑客常用的攻击平台是DOS(Disk Operating System，磁盘操作系统)，它采用命令提示符界面，直接运行系统中的命令提示符。在使用DOS时，所有的核心启动程序都被临时存储在内存中，用户可以随意使用。黑客在入侵的过程中会使用各种网络命令进行探测并获得信息，这些命令也是黑客入门最基本的要求。熟练使用这些命令，将为信息收集和安全防御带来极大便利。在这一任务里将介绍黑客常用的一些命令。

1.2 预备知识

1.2.1 网络安全简介

随着信息科技的迅速发展以及计算机网络的普及，计算机网络深入政府、军事、文教、金融、商业等诸多领域，可以说网络应用无处不在。资源共享和计算机网络安全一直作为一对矛盾体而存在着，计算机网络资源共享程度逐渐提高，信息安全问题也日益突出。

2012年1月16日，中国互联网信息中心(CNNIC)发布《第29次中国互联网络发展状况统计报告》。报告显示，截止2011年12月底，中国网民规模达到5.13亿，全年新增网民5580万。互联网普及率较上年提升4个百分点，达到38.3%。用手机上网的人数更是达到3.56亿，同比增长17.5%。中国网站规模达到229.6万，较上年增长20%，国家顶级域名.cn的注册量达到353万个，较2011年中增长26000多个。团购用户达到6465万，年增长高达244.8%。网络音乐、网络游戏和网络文学等娱乐应用的用户规模有小幅增长，但使用率

均有下滑。相比之下,网络视频的用户规模则较上一年增加 14.6%,达到 3.25 亿人,使用率提升至 63.4%。

网络应用已经渗透到现代社会生活的各个方面,包括电子商务、电子政务、电子银行等领域。由此,网络安全不仅成为商家关注的焦点,也是技术研究的热门领域,同时也是国家和政府的行为。信息安全空间成为传统的国界、领海、领空三大国防和基于太空的第四国防之外的“第五国防”。

国家计算机网络应急技术处理协调中心(简称 CNCERT/CC,其网站如图 1-1 所示)在 2012 年 7 月发布的《CNCERT 互联网安全威胁报告》中指出,2012 年 7 月我国基础网络运行总体平稳,未发生较大规模网络安全事件,但存在一定数量的针对互联网基础设施的拒绝服务攻击事件。政府网站和金融行业网站仍然是不法分子攻击的重点目标,安全漏洞是重要联网信息系统遭遇攻击的主要内因。在网络病毒活动情况方面,境内感染网络病毒的终端数约为 340 万个。其中,境内被木马或僵尸程序控制的主机 IP 约为 80 万个,按地区分布感染数量排名前三位的分别是广东省、江苏省和浙江省。境外木马或僵尸网络控制服务器 IP 数量为 7235 个,主要分布于美国、日本、韩国。全球互联网约 2208 万个主机 IP 感染飞客蠕虫,按国家感染数量排名前三位的分别是中国大陆、巴西、印度。境内感染飞客蠕虫的主机 IP 约为 260 万个;在捕获新增网络病毒文件中,按网络病毒名称统计新增 665 个,较上月大幅增长 50.5%,按网络病毒家族统计新增 12 个,较上月大幅增长 140.0%;在网站安全方面,被篡改网站数量为 1579 个,其中代号“残爱泪痕”、“左泪”和“Learner”的攻击者对境内网站进行了大量篡改。按地区分布排名前三位的分别是北京市、江苏省、广东省,被篡改数量最多的是.com 和.com.cn 域名类网站,被篡改的政府类网站数量为 193 个,占境内被篡改网站总数的 12.2%。境内被植入后门的网站数量为 5396 个,其中政府网站有 435 个,境外 2715 个 IP 通过植入后门对境内 3584 个网站实施远程控制,主要位于美国、韩国和印



图 1-1 “国家互联网应急中心”网站

尼等国家或地区。针对境内网站的仿冒页面数量为 1432 个，涉及域名 874 个，IP 地址 184 个；安全漏洞方面，国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞 596 个，其中高危漏洞 233 个，可被利用来实施远程攻击的漏洞有 548 个。受影响的软硬件系统厂商包括 Apache、Apple、Google、Cisco、HP、IBM、Linux、Microsoft、Mozilla、Symantec、WordPress 和 Oracle 等。按漏洞类型排名前三位的分别是应用程序漏洞、Web 应用漏洞、操作系统漏洞；垃圾邮件方面，共接收 6934 件垃圾邮件事件举报；事情受理方面，CNCERT 接收网络安全事件报告 1623 件，数量最多的分别是网页仿冒类事件 802 件、漏洞类事件 675 件。

1.2.2　黑客的定义

黑客是对英语 hacker 的翻译，hacker 原意是指用斧头砍柴的工人，最早被引进 IT 行业可追溯到 20 世纪 60 年代。黑客破解系统或者网络基本上认定为一项业余嗜好，通常是出于自己的兴趣，而非为了赚钱或工作需要。当时在麻省理工学院（MIT）中的学生通常分成两派，一派是 tool，意指“乖乖学生”，成绩都拿甲等；另一派则是所谓的 hacker，也就是常逃课、上课爱睡觉，但晚上精力充沛，喜欢搞课外活动的学生。真正的一流 hacker 并非整天不学无术，而是会热衷于追求某种特殊嗜好，比如研究电话、无线电，或者是计算机。也因此后来才有所谓的 computer hacker 出现，意指计算机高手。有些人很强调黑客和骇客的区别，认为黑客是有建设性的，骇客则专门搞破坏。对一名黑客来说，学会入侵和破解是必要的，但最主要的还是编程。对于一个骇客来说，他们只追求入侵的快感，不在乎技术；他们不会编程，不知道入侵的具体细节。还有一群人被称做“白帽黑客”或“匿名客”（sneaker）或“红客”，他们通常是计算机安全公司的雇员，并在完全合法的情况下攻击某系统。他们的工作是试图破解某系统或网络，以提醒该系统所有者系统的安全漏洞。

1.2.3　黑客的历史

黑客的早期历史可以追溯到 20 世纪五六十年代，麻省理工学院（MIT）率先研制出“分时系统”，学生们第一次拥有了自己的计算机系统。不久之后，学生们中出现了一批狂热分子，称自己是黑客，他们要彻底破坏大型主机的控制。

1961 年，拉塞尔的 3 位大学生编写了第一个游戏程序“空间大战”。其他学生也纷纷编写出更多好玩的游戏，比如象棋程序、留言软件等。他们属于第一代黑客，开发了大量有实用价值的应用程序。

20 世纪 60 年代中期，贝尔实验室的邓尼斯·里奇和肯·汤姆森编写出 UNIX 操作系统和 C 语言，推动了工作者计算机和网络的成长。MIT 的理查德·斯德尔曼成立了自由软件基金会，成为国际自由软件运动的精神领袖。他们是第二代黑客的代表人物。

1975 年，爱德华·罗伯茨发明第一台微型计算机。美国的计算机爱好者组织成立了“家庭酿造电脑俱乐部”，相互交流组装计算机的经验。他们属于第三代黑客。

1970 年，约翰·达帕尔利用口哨玩具开启电话系统，进行免费的长途通话。他因盗用电话线路而多次被捕。

1982 年，年仅 15 岁的凯文·米特尼闯入了北美空中防务指挥系统，这是首次发现的从外部入侵的网络事件。他后来连续进入美国多家大公司的计算机网络，1984 年向圣迭戈超级计算机中心发起攻击。他是著名的世界头号黑客，曾多次入狱，被指控偷窃了数以千计的

文件并非法使用多张信用卡。

1984 年,德国汉堡出现了混沌计算机俱乐部(CCC)。1987 年,CCC 的成员攻入了美国宇航局的 SPAN 网络。美国黑客戈德斯坦创办了著名的黑客杂志——*The Hack Quarterly*。

1988 年,美国康奈尔大学学生罗伯特·莫里斯向互联网释放蠕虫病毒,导致 10%以上的网络计算机同时出现故障,造成用户直接经济损失近 1 亿美元。

1995 年,俄罗斯黑客列文在英国被捕。他被指控从纽约花旗银行非法转移至少 370 万美元。

1999 年,美国黑客戴维·史密斯制造了梅丽莎病毒,通过互联网在全球感染数百万台计算机和数万台服务器。

2000 年,全世界黑客联手发动的黑客战争袭击了互联网最热门的八大网站,包括 Yahoo 和微软,造成网站瘫痪数小时,造成经济损失 17 亿美元。菲律宾学生奥内尔·古兹曼制造了爱虫病毒,因感染该病毒使计算机瘫痪造成的经济损失高达 100 亿美元。

1.2.4 端口概述

端口是计算机与外界通信交流的出口。根据端口的性质,可以分为以下 3 类。

(1) 公认端口,也称为"常用端口",范围为 0～1023,它们紧密绑定于一些特定的服务。通常,这些端口的通信能够明确地表明某种服务的协议。这种端口是不可以被其他协议占用的。例如,21 端口就是 FTP(文件传输协议)的端口,23 号端口是 Telnet 服务专用的,而 80 端口实际是 HTTP 通信所使用的。这些端口通常不会被黑客程序利用。

(2) 注册端口的范围是 1024～49151。它们分散地绑定于一些服务,也就是说,有很多服务绑定于这些端口。这些端口同样用于许多其他目的,大多数没有明确的定义服务对象,不同的程序可以根据实际需要自行定义。

(3) 动态和私有端口号的范围是 49152～65535,理论上不应该把常用服务分配在这些端口上。但实际上有些较为特殊的程序,特别是一些木马程序,就非常喜欢用这些端口,因为这些端口一般不被注意,非常容易隐蔽。

1.3 方案设计

方案设计如表 1-1 所示。

表 1-1 方案设计

任务名称	了解常见黑客命令
任务分解	1. 扫描开放的端口 (1) 使用 netstat 命令查看 (2) 使用 fport 工具查看 (3) 使用 Active Ports 工具查看 2. 黑客常用的入侵命令 (1) net 命令的使用 (2) tracert 命令的使用 (3) route 命令的使用

续表

能力目标	1. 能使用 netstat 命令查看网络状态 2. 能使用 fport 工具在命令行窗口查看系统当前打开的端口、进程等信息 3. 能使用 Active Ports 工具查看本地计算机的开放端口信息 4. 能使用 net user 命令显示、修改、添加或删除账户 5. 能使用 net localgroup 命令提升、降低账户权限 6. 能使用 net share 命令创建、删除共享资源 7. 能使用 net start/stop 命令启动、停止 Windows 网络服务 8. 能使用 net send 命令向网络的其他用户、计算机发送消息 9. 能使用 net view 命令显示域列表、计算机列表或指定计算机共享资源列表 10. 能使用 tracert 命令确定 IP 数据包访问目标所通过的路径 11. 能使用 route 命令查看、添加、修改和删除路由条目
知识目标	1. 了解网络安全的重要意义 2. 熟悉黑客的定义 3. 了解黑客的发展历史 4. 熟悉黑客入侵的一般过程 5. 了解端口的作用和分类
素质目标	1. 掌握网络安全行业的基本情况 2. 培养良好的职业道德 3. 培养创新能力 4. 树立较强的安全、节约、环保意识 5. 培养良好的沟通与团队协作能力

1.4 任务实施

一般来说，黑客对计算机进行攻击的步骤大致相同，主要包括扫描漏洞、试探漏洞、取得权限与提升权限、木马入侵、建立后门与清理痕迹。其中，扫描系统开放的端口、创建用户、提升用户权限等操作均可以使用系统自带命令完成。

1.4.1 任务 1：扫描开放的端口

1. 任务目标

熟练掌握使用系统自带命令 netstat 命令查看网络连接情况，熟悉使用第三方工具 fport 工具和 Active Ports 工具扫描系统开放的端口信息。

2. 工作任务

(1) 使用 netstat 命令查看；

(2) 使用 fport 工具查看；

(3)使用 Active Ports 工具查看。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机，通过网络相连。

(2) 软件工具：fport、Active Ports。

4. 实施过程

(1) 使用 netstat 命令查看

netstat 命令用来查看网络状态，其操作简便，功能强大，主要用于显示与 IP、TCP、UDP 以及 ICMP 有关的统计数据，一般用于检验本机与远程计算机各端口的网络连接情况。

netstat 的命令格式为

```
netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

其中，选项[-a]用于显示活动的 TCP 连接、侦听端口；选项[-e]用于显示以太网统计的信息；选项[-s]用于显示按协议统计的信息；选项[-r]用于显示路由表内容；选项[-p]用于显示指定协议的连接。

命令中各参数的操作如下：

① 选择"开始"→"运行"菜单项，打开"运行"对话框，在"打开"下拉列表文本框中输入"cmd"，然后单击"确定"按钮。

② 在打开的命令提示符窗口中输入"netstat -an"，按"Enter"键即可查看本地计算机所开放的端口信息，如图 1-2 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12071          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1030         0.0.0.0:0              LISTENING
  TCP    192.168.75.5:139       0.0.0.0:0              LISTENING
  TCP    192.168.75.5:3036      112.90.138.230:80      TIME_WAIT
  TCP    192.168.75.5:3037      58.251.60.173:80       TIME_WAIT
  TCP    192.168.139.1:139      0.0.0.0:0              LISTENING
  TCP    192.168.190.1:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:80             *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1034           *:*
```

图 1-2 "netstat -an"窗口

③ 在打开的命令提示符窗口中输入"netstat -a"，按"Enter"键即可查看所有连接和监听端口，如图 1-3 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    20090326-1043:epmap    20090326-1043:0        LISTENING
  TCP    20090326-1043:microsoft-ds  20090326-1043:0        LISTENING
  TCP    20090326-1043:12071    20090326-1043:0        LISTENING
  TCP    20090326-1043:1030     20090326-1043:0        LISTENING
  TCP    20090326-1043:netbios-ssn  20090326-1043:0        LISTENING
  TCP    20090326-1043:3036     112.90.138.230:http    TIME_WAIT
  TCP    20090326-1043:3037     reverse.gdsz.cncnet.net:http  TIME_WAIT
  TCP    20090326-1043:netbios-ssn  20090326-1043:0        LISTENING
  TCP    20090326-1043:netbios-ssn  20090326-1043:0        LISTENING
  UDP    20090326-1043:80       *:*
  UDP    20090326-1043:microsoft-ds  *:*
  UDP    20090326-1043:1034     *:*
```

图 1-3 "netstat -a"窗口

④ 在打开的命令提示符窗口中输入“netstat -b”，按“Enter”键即可查看包含于每个连接或监听端口的可执行组件，如图 1-4 所示。

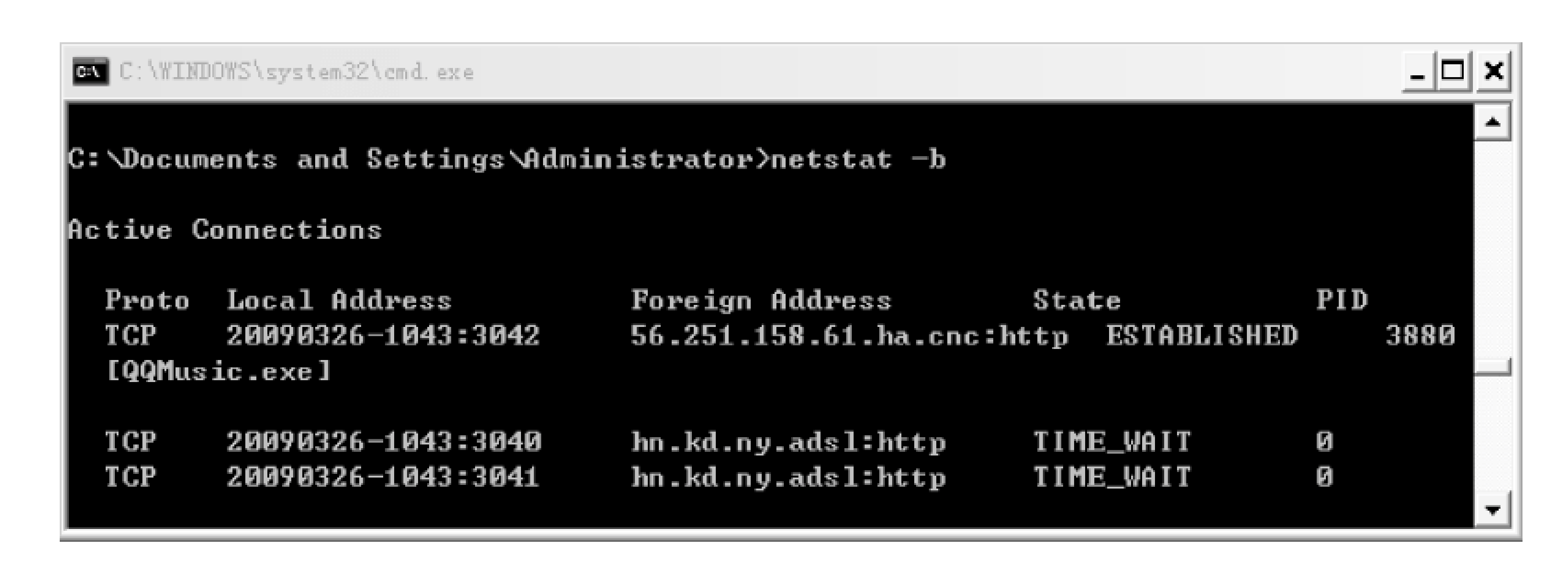


图 1-4　“netstat -b”窗口

⑤ 在打开的命令提示符窗口中输入“netstat -e”，按“Enter”键即可查看以太网数据统计信息，可以与-s 参数结合使用，如图 1-5 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      69547742         8833104
Unicast packets               81513           88003
Non-unicast packets            1579             153
Discards                          0               0
Errors                            0               0
Unknown protocols                51
```

图 1-5　“netstat -e”窗口

⑥ 在打开的命令提示符窗口中输入“netstat -n”，按“Enter”键即可查看以网络 IP 地址代替名称的网络连接情形，如图 1-6 所示。

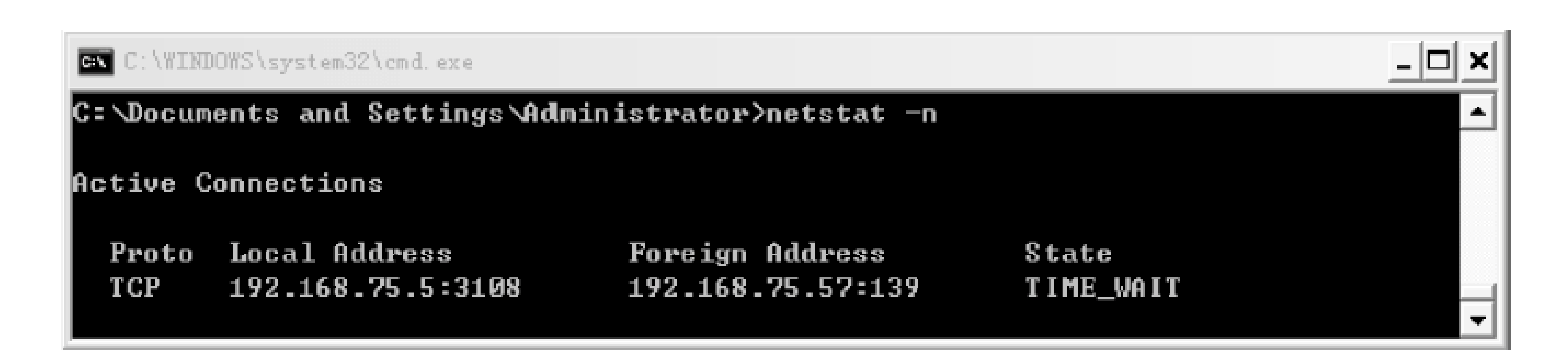


图 1-6　“netstat -n”窗口

⑦ 在打开的命令提示符窗口中输入“netstat -o”，按“Enter”键即可查看与每个连接相关的所属进程 ID，如图 1-7 所示。

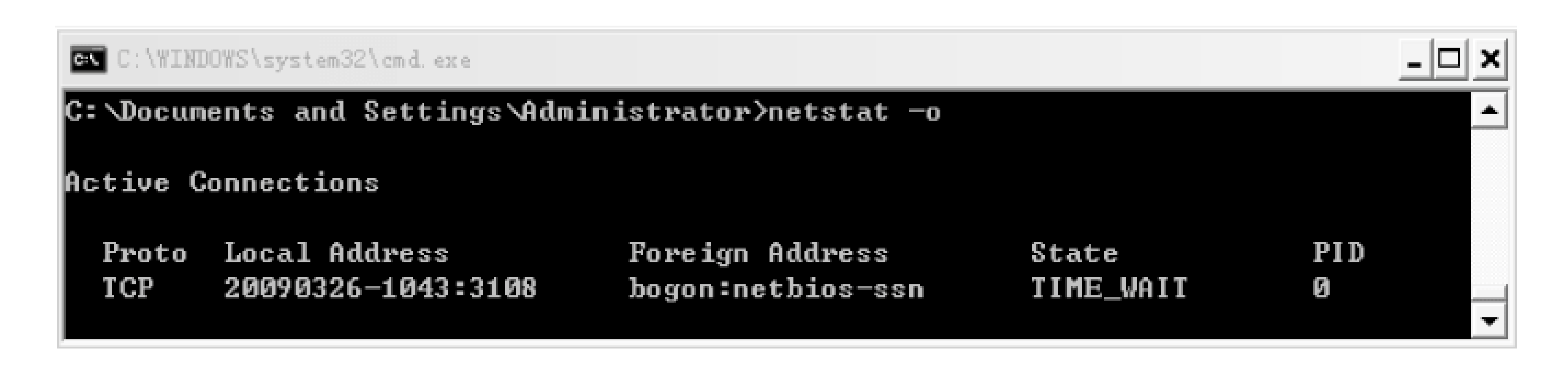


图 1-7　“netstat -o”窗口

⑧ 在打开的命令提示符窗口中输入“netstat -p pro”，pro 可以是 tcp 或 udp，按“Enter”键即可查看 pro 指定协议的连接信息，如图 1-8 所示。

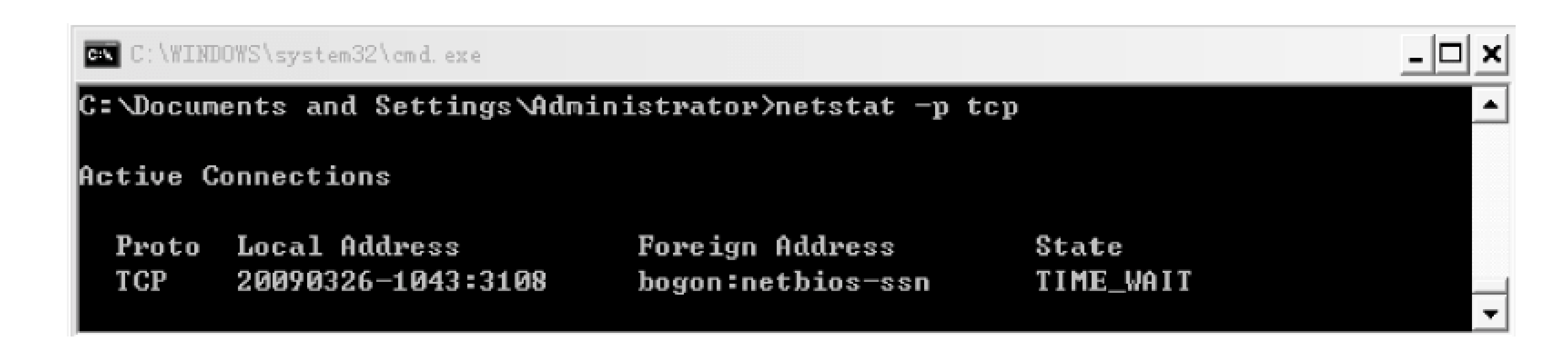


图 1-8 “netstat -p tcp”窗口

⑨ 在打开的命令提示符窗口中输入“netstat -r”，按“Enter”键即可查看路由表信息，如图 1-9 所示。

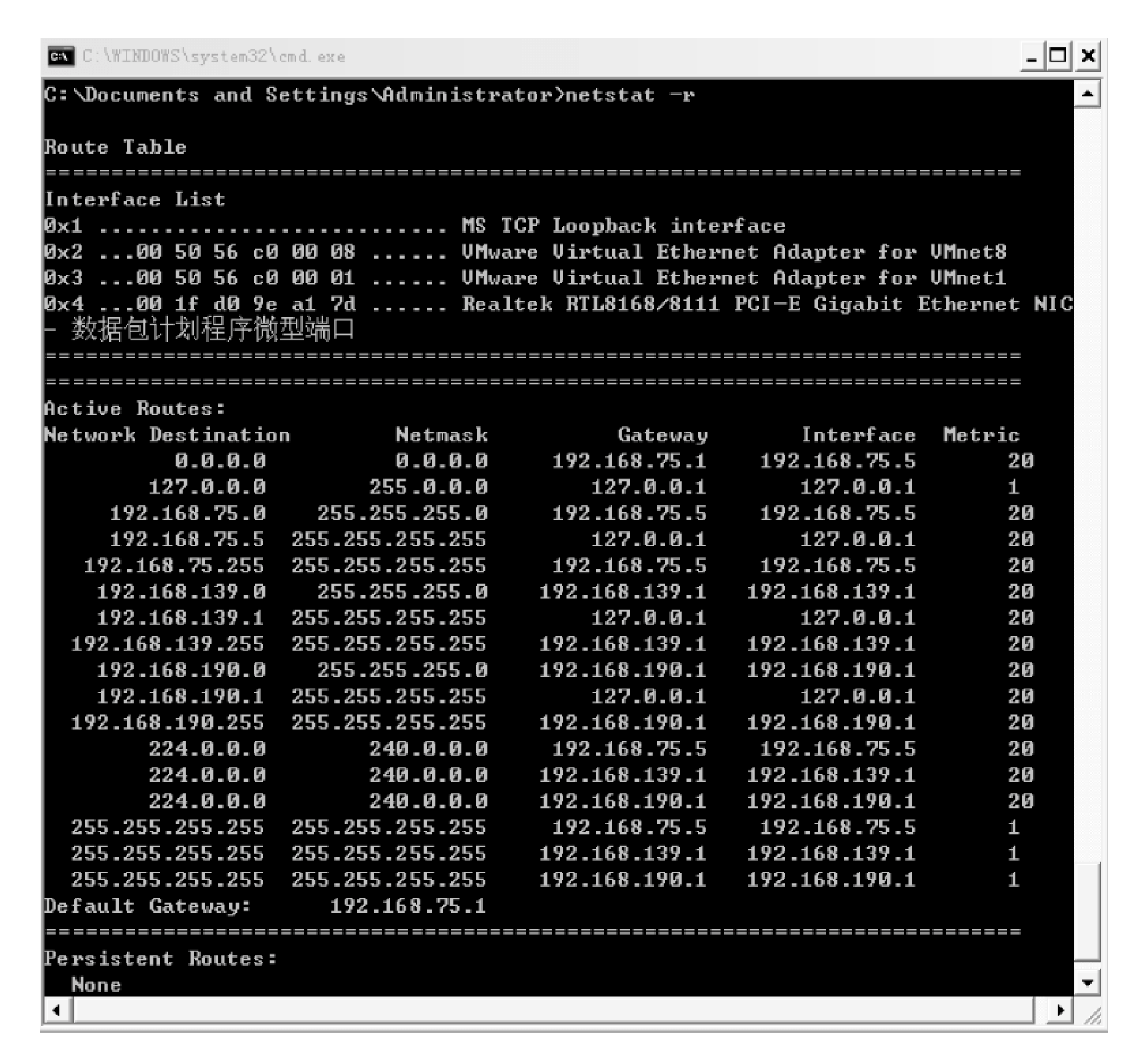


图 1-9 “netstat -r”窗口

⑩ 在打开的命令提示符窗口中输入“netstat -s”，按“Enter”键即可查看每个协议的配置统计，包括 TCP、IP、UDP、ICMP 等协议，可以与-e 参数结合使用，如图 1-10 所示。

(2) 使用 fport 工具查看

使用 fport 工具可以将系统中当前打开的 TCP/IP 和 UDP 端口显示出来，还能查看与端口对应的软件的路径和进程名称等。使用 fport 工具查看本地计算机开放的端口信息的具体操作如下：

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。

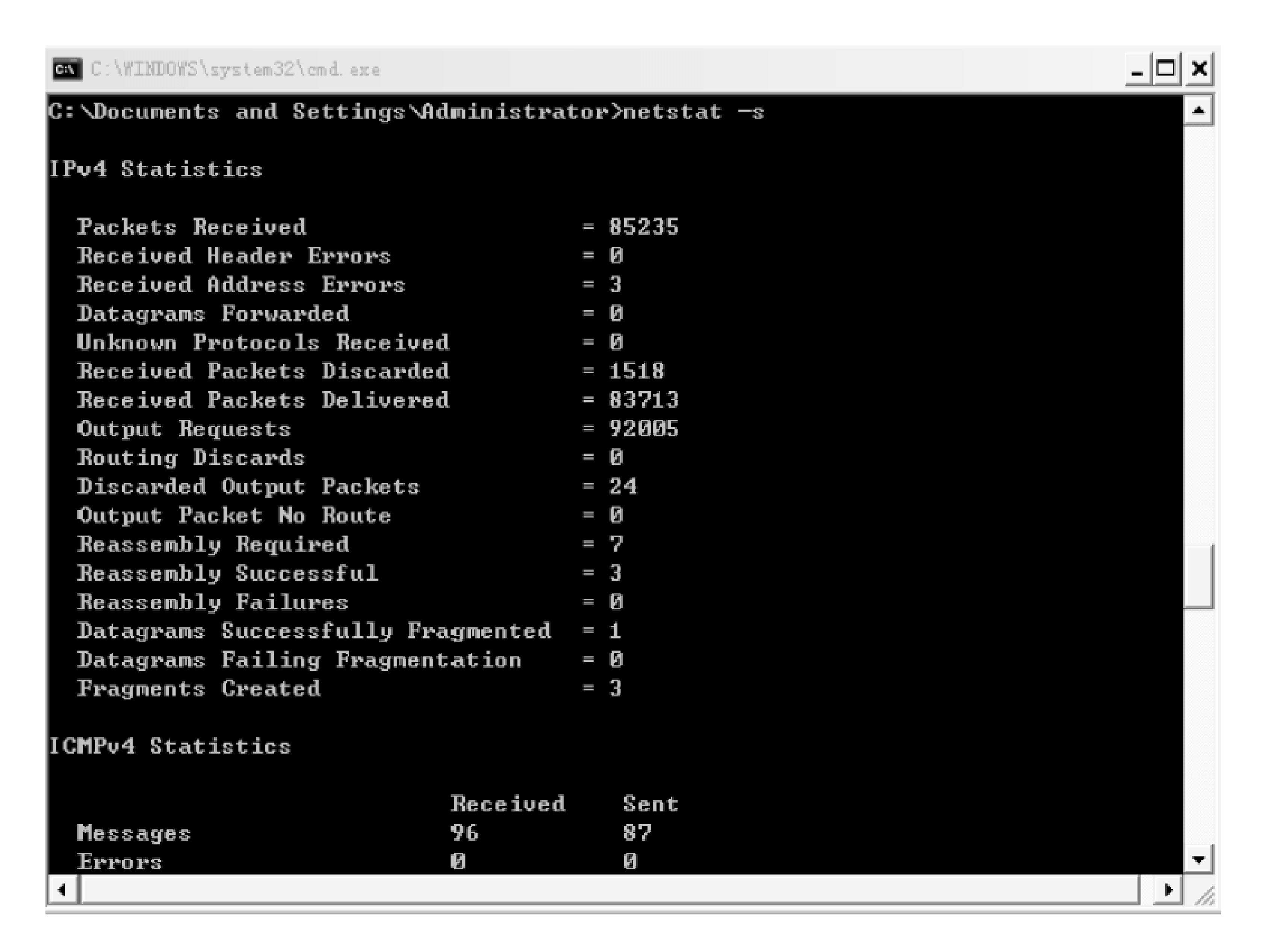


图 1-10　“netstat -s”窗口

② 打开命令提示符窗口，使用 DOS 命令进入 fport 工具所在的目录，然后输入“fport”命令，按“Enter”键即可启动 fport 工具。

③ fport 工具将自动扫描本地计算机所开放的端口和使用该端口的相应应用程序，并将其显示出来，如图 1-11 所示。

```
C:\WINDOWS\system32\cmd.exe
D:\fport>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
1240                 ->  135   TCP
4     System         ->  139   TCP
4     System         ->  445   TCP
3188                 ->  1030  TCP
1268                 ->  3269  TCP
3880  QQMusic        ->  12071 TCP   C:\Program Files\Tencent\QQMusic\QQMusic.ex
e

1240                 ->  80    UDP
0     System         ->  123   UDP
3596  QQ             ->  123   UDP   C:\Program Files\Tencent\QQ\bin\QQ.exe
```

图 1-11　“fport 工具”窗口

(3) 使用 Active Ports 工具查看

使用命令提示符窗口查看端口信息较为复杂，使用 Active Ports 工具查看则简单得多。使用 Active Ports 工具查看本地计算机开放的端口信息的具体操作如下：

① 安装 Active Ports 工具，步骤比较简单，不再赘述。

② 选择“开始”→“所有程序”→“Active Ports”命令，启动 Active Ports 工具软件。

③ 在打开的 Active Ports 窗口中可以看到当前系统所开放的端口以及这些端口所对应的应用程序，如图 1-12 所示。

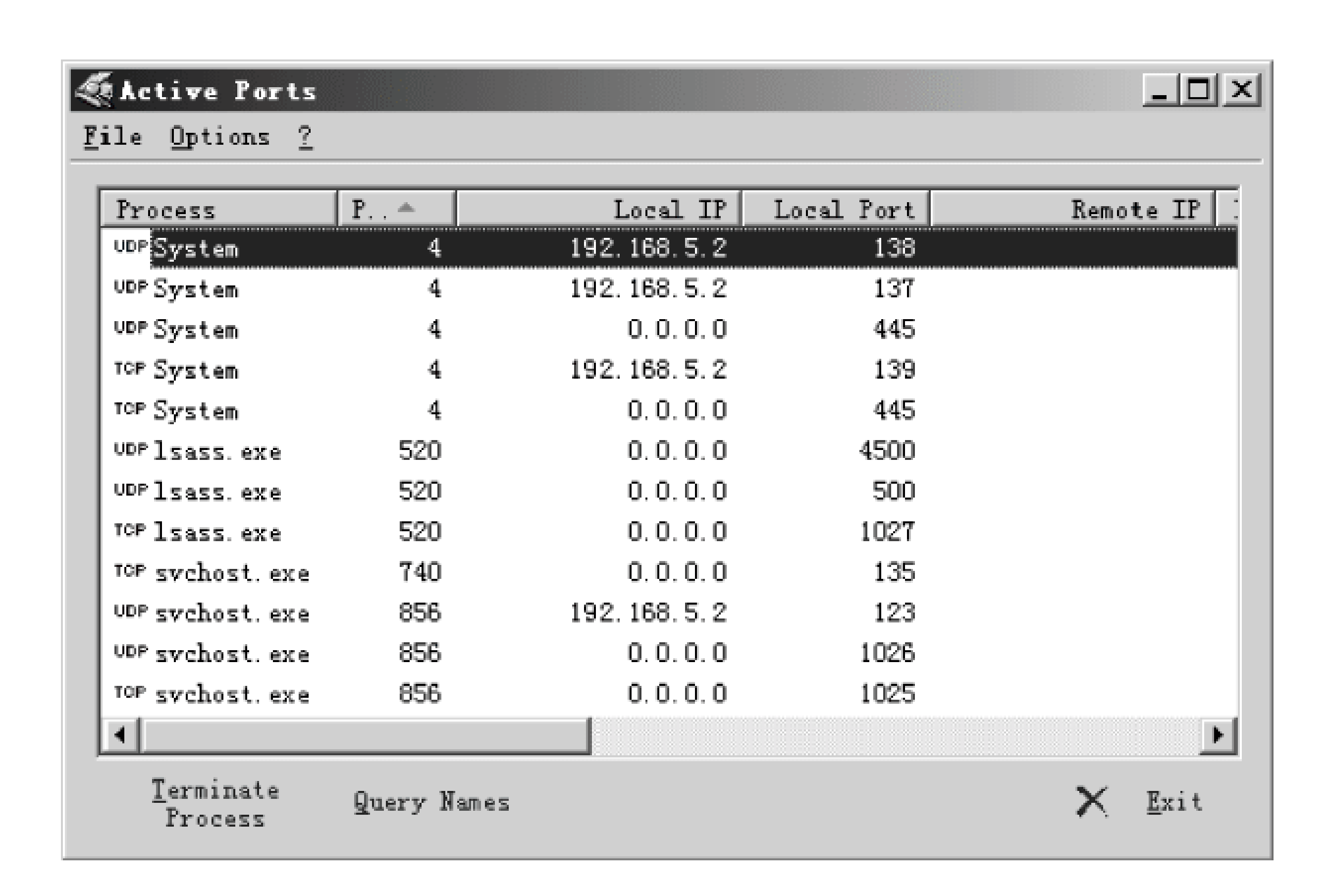


图 1-12 “Active Ports 工具”窗口

1.4.2 任务 2：黑客常用的入侵命令

1. 任务目标

熟练掌握使用 net 命令完成以下操作：显示、修改、添加或删除账户；提升、降低账户权限；创建、删除共享资源；启动、停止 Windows 网络服务；向网络的其他用户、计算机发送消息；显示域列表、计算机列表或指定计算机共享资源列表。能熟练使用 tracert 命令确定 IP 数据包访问目标所通过的路径；使用 route 命令查看、添加、修改和删除路由条目。

2. 工作任务

(1) net 命令的使用；

(2) tracert 命令的使用；

(3) route 命令的使用。

3. 工作环境

两台预装 Windows Server 2003/XP 的主机，通过网络相连。

4. 实施过程

1) net 命令的使用

net 命令功能强大，以命令行方式执行，使用它可以轻松地管理本地或远程计算机的网络环境以及各种服务程序的运行和配置。它还包括多个不同的附加命令，通过这些命令可以实现添加、删除、显示本地组，连接计算机或共享资源，启动、停止服务，添加、删除用户账户，提升或降低用户权限等各种重要功能。下面介绍 net 命令中一些常用命令的基本功能。

(1) net user 命令

该命令主要用来显示账户信息，修改、添加或删除账户。

下面以创建一个名为“a”的受限账户，然后将其删除为例，介绍 net user 命令的使用方法。

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。

② 首先创建一个名为“a”的受限账户。在命令提示符窗口输入“net user a 123 /add”命

令，然后按“Enter”键，即创建一个名为“a”、密码为“123”的受限账户，如图 1-13 所示。



图 1-13　添加账户

③ 打开“计算机管理”的本地用户和组，即可看到刚创建的受限账户，如图 1-14 所示。



图 1-14　查看受限账户

④ 如果用户想要将该账户提升为管理员账户，可以在命令提示符窗口中输入“net localgroup administrators a /add”命令，然后按“Enter”键，如图 1-15 所示。

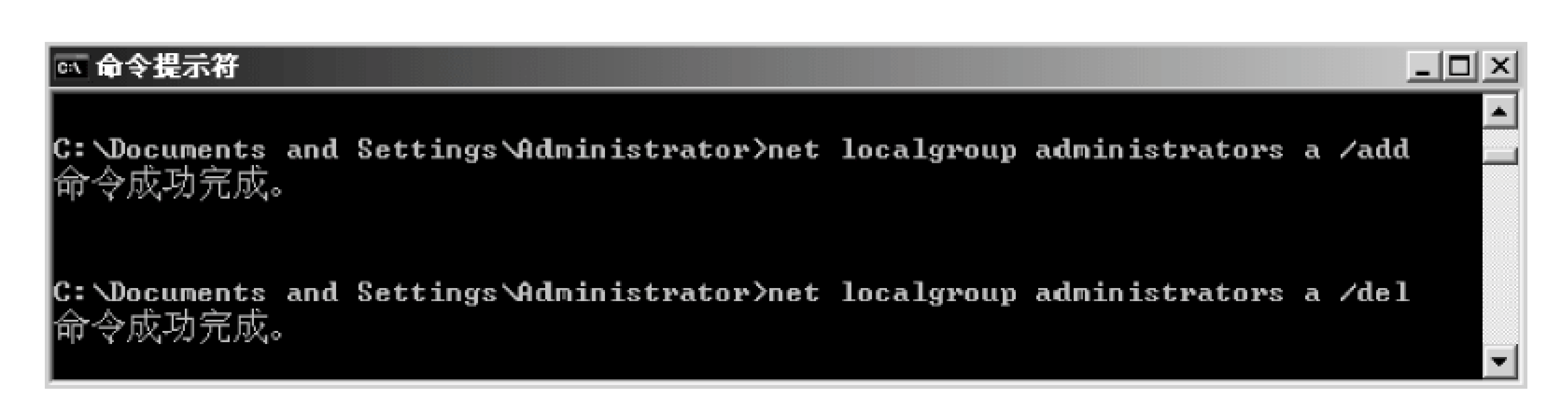


图 1-15　提升和降低账户权限

⑤ 打开“计算机管理”查看该账户的属性，可看到账户 a 已经隶属于管理员账户组，如图 1-16 所示。

⑥ 如果用户想要将该账户降级为受限账户，可以在命令提示符窗口中输入“net localgroup administrators a /del”命令，然后按“Enter”键。此时打开“计算机管理”查看该账户的属性，可看到账户 a 重新仅属于 users 组，如图 1-17 所示。

⑦ 如果用户想要删除刚才创建的账户，可以在命令提示符窗口中输入“net user a /del”命令，然后按“Enter”键，即可将创建的“a”账户删除。此时在“计算机管理”的本地用户和组里就看不到刚创建的受限账户 a 了。

（2）net share 命令

该命令的作用是创建、删除共享资源。

下面以将本地磁盘 C 设为最多允许 60 人访问的共享磁盘为例，介绍 net share 命令的使用方法。



图 1-16　查看账户属性(1)



图 1-17　查看账户属性(2)

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。

② 首先将本地磁盘 C 共享，并设置最大共享人数为 60 人。在命令提示符窗口输入“net share c=c：/user:60”命令，然后按“Enter”键，即可将本地磁盘 C 设为最多允许 60 人访问的共享磁盘，如图 1-18 所示。



图 1-18　共享 C 盘命令

③ 在“我的电脑”窗口中右击，然后从弹出的快捷菜单中选择“刷新”菜单项可以查看结果，此时在磁盘 C 图标上有一只“小手”，如图 1-19 所示。



图 1-19　C 盘共享

④ 如果想要取消本地磁盘 C 的共享，可以在命令提示符窗口中输入“net share c /del”命令，然后按“Enter”键。

⑤ 如果要将本地磁盘 D 设置为隐藏共享，可打开命令提示符窗口，然后输入“net share d$ =d:”命令，再按“Enter”键，如图 1-20 所示，即可将本地磁盘 D 设为隐藏的共享磁盘。即在“我的电脑”窗口中右击，从弹出的快捷菜单中选择“刷新”菜单项后也看不到 D 盘图标共享的“小手”。只有在命令提示符下输入“net share”命令，然后按下“Enter”键，才可以看到隐藏的共享磁盘 D，如图 1-21 所示。



图 1-20　D 盘隐藏共享



图 1-21　查看共享磁盘

⑥ 如果想要取消本地磁盘 D 的隐藏共享，可以在命令提示符窗口中输入“net share d$ /del”命令，然后按“Enter”键。这时，在命令提示符下输入“net share”命令，然后按下“Enter”键，可以看到磁盘 D 没有隐藏共享了，如图 1-22 所示。



图 1-22　删除 D 盘隐藏共享

(3) net start/stop 命令

该命令的作用是启动/停止 Windows 网络服务，格式为

net start/stop [service]

下面以启动信使服务为例，介绍 net start 命令的使用方法。

① 禁用的服务不能用 net start 命令开启，否则会出现如图 1-23 所示的错误提示。



图 1-23　错误提示

② 选择“开始”→“所有程序”→“管理工具”→“服务”命令，启动“服务”窗口，可以看到“Messenger”服务的启动类型是“禁用”，如图 1-24 所示。



图 1-24　查看“Messenger”服务的启动类型

③ 右击“Messenger”服务的属性菜单项，打开“Messenger 的属性(本地计算机)”对话框，把启动类型设置为“自动”或“手动”，然后单击“确定”按钮，如图 1-25 所示。



图 1-25　设置启动类型为“自动”

④ 选择“开始”→“运行”菜单项，打开“运行”对话框，在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。

⑤ 在命令提示符窗口输入“net start messenger”命令，然后按“Enter”键，即可启动信使服务，如图 1-26 所示。

```
命令提示符
C:\Documents and Settings\Administrator>net start messenger
Messenger 服务正在启动 ....
Messenger 服务已经启动成功。
```

图 1-26　启动信使服务

⑥ 在命令提示符窗口输入“net stop messenger”命令，然后按“Enter”键，即可停止信使服务，如图 1-27 所示。



图 1-27　停止信使服务

（4） net send 命令

该命令的作用是向网络的其他用户、计算机发送消息。要接收消息，必须运行信使服务。

下面以计算机 A 向计算机 B(IP 地址为 192.168.5.1)的主机发送消息“hello!”为例，介绍 net send 命令的使用方法。

① 在计算机 B 的命令提示符窗口中输入“net start messenger”命令，然后按“Enter”键，启动信使服务。

② 在计算机 A 的命令提示符窗口输入“net send 192.168.5.1 hello!”命令，然后按“Enter”键，显示消息已经送到计算机 B，如图 1-28 所示。



图 1-28　发送消息

③ 在计算机 B 上接收到来自计算机 A(GL-VM1) 的消息，如图 1-29 所示。

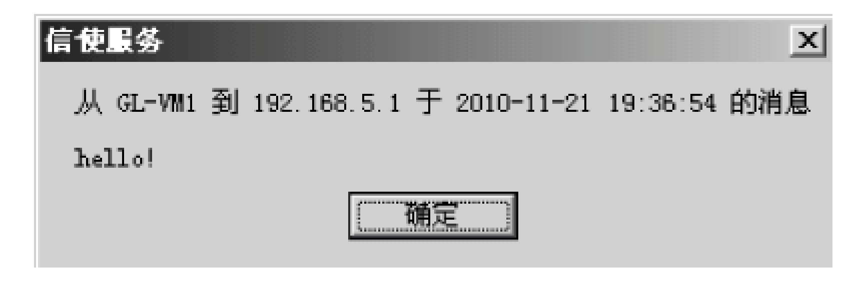


图 1-29　收到消息

（5） net view 命令

该命令的作用是显示域列表、计算机列表或指定计算机共享资源列表。

下面以计算机 A 查询计算机 B 的共享资源列表为例，介绍 net view 命令的使用方法。

① 在计算机 A 的命令提示符窗口中输入“net view 192.168.5.1”命令，然后按“Enter”键，即可查看到计算机 B 中的共享资源，如图 1-30 所示。

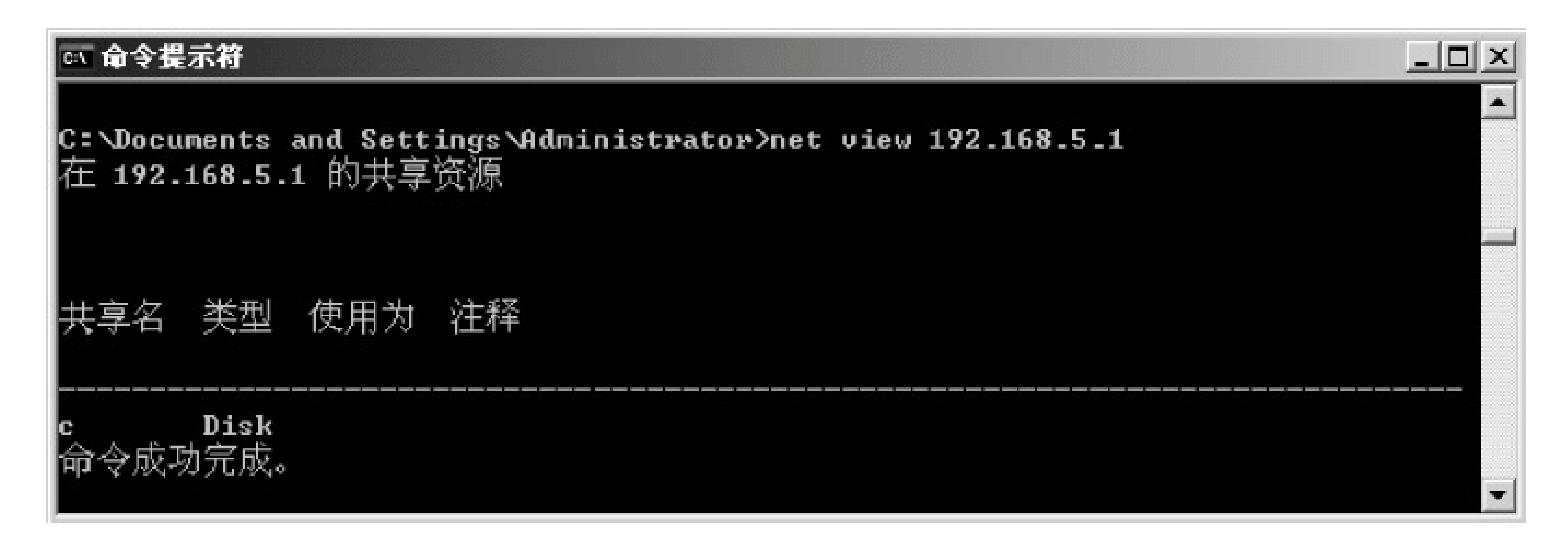


图 1-30 查看共享资源

② 在计算机 A 的命令提示符窗口中输入“net view”命令，然后按“Enter”键，即可显示计算机 A 的当前域中的计算机列表。

2）tracert 命令的使用

tracert 命令是路由跟踪实用程序，用于确定 IP 数据包访问目标所通过的路径。tracert 命令通过发送包含不同 IP 生存时间字段 TTL 的 ICMP 超时通告报文并监听回应报文来确定从一台主机到网络上其他主机的路由。tracert 命令的格式为

tracert [-d] [-h maxmum_hops] [-j host-list] [-w timeoute] target_name

其中，[-d]表示不把 IP 地址解析成域名；[-h maxmum_hops]表示允许跟踪的最大跳数；[-j host-list]表示经过的主机列表；[-w timeoute]表示每次恢复的最大允许延时。

利用 tracert 命令搜索网站结构信息的具体操作如下：

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。

② 在命令提示符窗口输入“tracert www. sina. com. cn”命令，然后按“Enter”键，即可在返回的结果中获知数据包经过了哪些节点，如图 1-31 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>tracert www.sina.com.cn

Tracing route to libra.sina.com.cn [202.108.33.92]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  bogon [192.168.75.1]
  2    <1 ms    <1 ms    <1 ms  192.168.253.254
  3     1 ms     1 ms     1 ms  221.4.148.241
  4     1 ms     1 ms     1 ms  120.80.205.161
  5     2 ms     2 ms     2 ms  120.80.0.241
  6     2 ms     2 ms     2 ms  219.158.19.9
  7    52 ms    36 ms    35 ms  219.158.14.37
  8    35 ms    35 ms    35 ms  123.126.0.162
  9    44 ms    44 ms    44 ms  61.148.143.26
 10    42 ms    42 ms    42 ms  210.74.176.138
 11    34 ms    34 ms    34 ms  202.108.33.92

Trace complete.
```

图 1-31 搜索网站结构信息

如果已经知道了局域网内某个目标主机的名称，可以使用 tracert 命令来获取该主机的 IP 地址；也可以通过 tracert 命令追踪那些神秘网友的 IP 地址，了解其中都经过了哪些中

转站。

3）route 命令的使用

route 命令一般用于管理本地计算机的路由表，使用它可以查看、添加、修改和删除路由表条目，还可以查看本地计算机的 IP 信息。该命令只有在安装了 TCP/IP 之后才能使用。route 命令的格式为

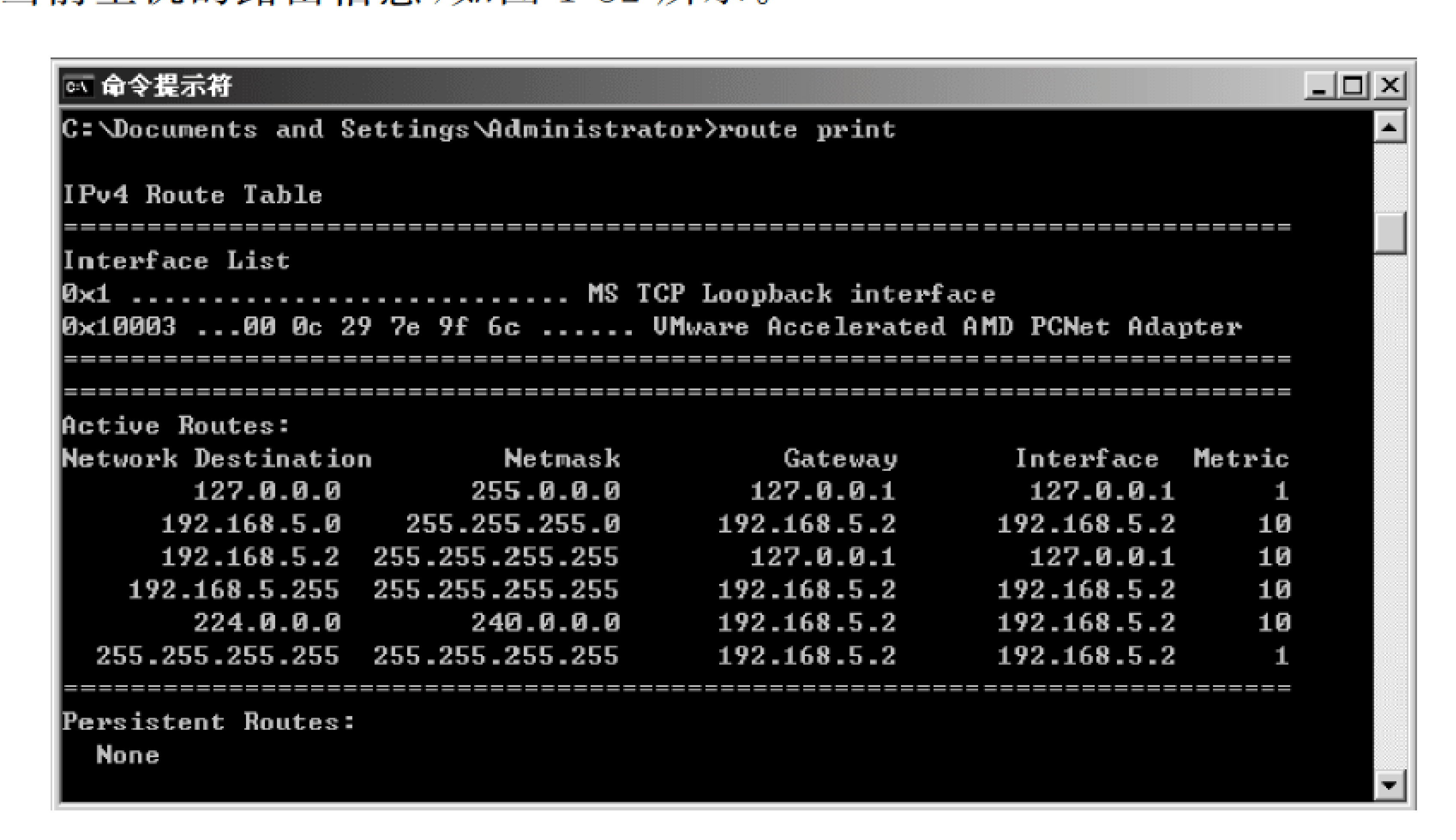
route [-f] [-p] [command] [destination] [mask subnetmask] [gateway] [metric metric] [if interface]

其中，[-f]表示清除路由表中所有的网关条目；[command]可以是 add、delete 和 print，分别表示添加路由表条目、删除路由表条目和列出当前路由表条目；[-p]与命令 add 一起使用时，将使增加的路由表项永久有效，即使重新启动系统。

使用 route 命令查看本地 IP 信息的具体操作如下：

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。

② 在命令提示符窗口输入“route print”命令，然后按“Enter”键，即可在命令提示符窗口中显示当前主机的路由信息，如图 1-32 所示。



```
命令提示符
C:\Documents and Settings\Administrator>route print

IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 0c 29 7e 9f 6c ...... VMware Accelerated AMD PCNet Adapter
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
        192.168.5.0    255.255.255.0      192.168.5.2     192.168.5.2      10
        192.168.5.2  255.255.255.255        127.0.0.1       127.0.0.1      10
      192.168.5.255  255.255.255.255      192.168.5.2     192.168.5.2      10
          224.0.0.0        240.0.0.0      192.168.5.2     192.168.5.2      10
    255.255.255.255  255.255.255.255      192.168.5.2     192.168.5.2       1
===========================================================================
Persistent Routes:
  None
```

图 1-32　显示路由信息

路由表中的 Destination、Netmask、Gateway、Interface 和 Metric 参数分别指定路由表条目中的目标 IP、子网掩码、使用网关、度量值和网络接口。

1.5　常见问题解答

1. fport 工具和命令行方式查看端口信息有何不同？

答：使用 fport 工具查看端口信息比使用命令查看到的信息更详尽，也更有利于用户进行判断。

2. 如何利用 Active Ports 软件关闭端口？

答：Active Ports 软件提供了关闭端口的功能，只需选择相应的进程，然后单击“Terminate process”按钮即可。

3. 怎样确定计算机资源共享成功了?

答：有两种方法验证是否共享成功，第一种方法是使用“net share”命令进行查看；第二种方法是打开“我的电脑”窗口进行验证，会看到C盘图标下有一只“手”，如果没有看到，可以右击并从弹出的快捷菜单中选择“刷新”，即可看到。

4. 忘记系统的登录密码怎么办?

答：下面以恢复本地用户“magic”口令为例，说明解决忘记登录密码的问题的步骤。重新启动计算机，在启动画面出现后马上按下F8键，然后选择“带命令行的安全模式”。运行过程结束时，系统列出了系统超级用户administrator和本地用户magic的选择菜单，用鼠标单击administrator进入命令行模式，然后输入命令“net user magic 123456 /add”，强制将magic的用户口令更改为123456。若想在此添加一个新用户(如用户名为abc，口令为123)，请输入“net user abc 123 /add”，再用“net localgroup administrators abc /add”命令将用户提升为管理员组administrators的成员，并使其具有超级权限。

5. arp命令有什么用?

答：地址解析协议(Address Resolution Protocol，ARP)是TCP/IP协议簇网络层的一个协议，为每个网络节点建立IP地址与MAC地址之间的对应(映射)关系。命令arp用于显示和修改地址解析协议(ARP)缓存中的项目。选项[-a]用于显示所有接口的当前ARP表项；选项[-s]用于添加一个静态ARP表项，将某个IP地址与MAC地址关联；选项[-d]用于删除指定的ARP表项。当网络感染ARP木马时，主机或网关所对应的MAC地址被修改，可执行arp -d清除ARP缓存表，再使用arp -s命令重新绑定正确的IP地址与MAC地址对。

1.6 过关练习

一、选择题

1. 在Windows操作环境中，采用(　　)命令来查看本机IP地址及网卡MAC地址。

A. ping　　B. tracert　　C. netstat　　D. ipconfig

2. 某客户端采用ping命令检测网络连接故障时，发现可以ping通127.0.0.1及本机的IP地址，但无法ping通同一网段内其他工作正常的计算机的IP地址，该客户端的故障可能是(　　)。

A. TCP/IP协议不能正常工作　　B. 本机网卡不能正常工作

C. 本机网络接口故障　　D. 本机DNS服务器地址设置错误

3. 下面关于ICMP协议的描述中，正确的是(　　)。

A. ICMP协议根据MAC地址查找对应的IP地址

B. ICMP协议把公网的IP地址转换为私网的IP地址

C. ICMP协议根据网络通信的情况把控制报文发送给发送方主机

D. ICMP协议集中管理网络中的IP地址分配

4. 在Windows操作系统中，如果要查找从本地出发，经过3个跳步，到达名字为Sdpt的目标主机的路径，则输入的命令是(　　)。

A. tracert Sdpt -h 3　　B. tracert -j 3 Sdpt

C. tracert -h 3 Sdpt　　D. tracert Sdpt -j 3

5. 能显示 TCP 和 UDP 连接信息的命令是(　　)。

A. netstat -s　　B. netstat -e　　C. netstat -r　　D. netstat -a

二、填空题

FTP 协议使用________端口，Telnet 协议使用________端口，SMTP 协议使用________端口，POP3 协议使用________端口，HTTP 协议使用________端口，DNS 协议使用________端口，QQ 使用________端口。

三、简答题

1. 一般系统攻击有哪些步骤？各步骤主要完成什么工作？
2. 什么是端口？如何查看本地计算机端口的开放情况？

四、实操题

1. 在自己的计算机上使用 netstat 命令查看网络状况。
2. 下载并安装 Active Ports 工具，查看自己计算机上的端口信息。
3. 使用 tracert 命令追踪百度网站(www.baidu.com)的 IP 信息。

工作任务二

目标系统的探测

21 用户需求与分析

目标主机信息收集的方法有两种：一种是使用各种扫描工具对目标主机进行大规模的扫描，得到系统信息和运行的服务信息；另一种是利用各种查询手段得到与目标主机相关的一切信息。目前大部分计算机安装的是 Windows 操作系统，尽管该系统的稳定性和安全性随着版本的提升而不断提高，但仍难免会出现这样或那样的安全隐患，这些安全隐患就是漏洞。黑客通过对目标系统进行扫描发现这些漏洞，然后使用病毒和木马攻击这些漏洞和破坏计算机系统。在了解目标主机的漏洞和弱点后，黑客甚至能探测出目标主机用户账号和密码等信息，从而达到试探性攻击的目的。

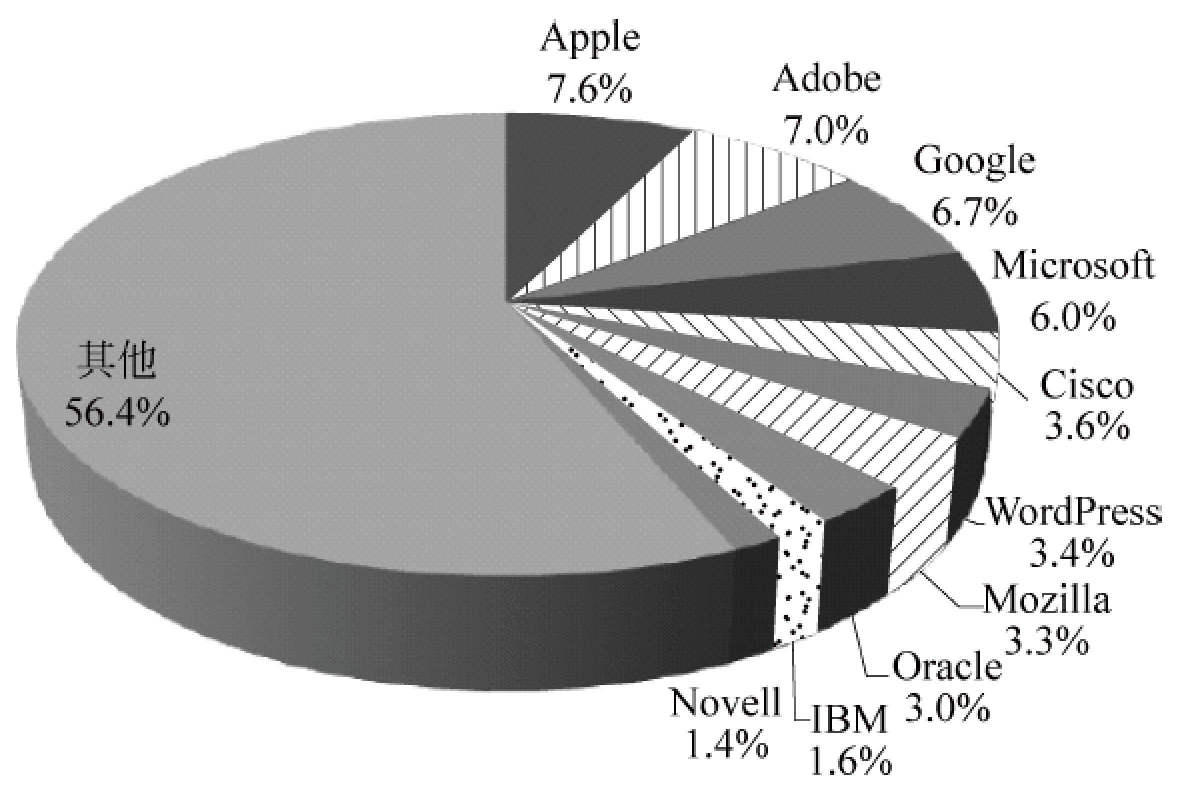
22 预 备 知 识

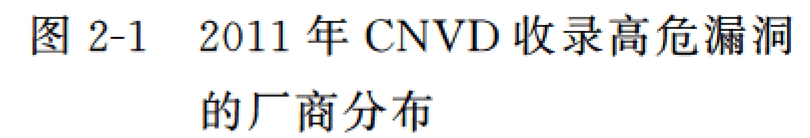
2.2.1 漏洞概述

由于大部分严重的网络安全威胁都是由信息系统所存在的安全漏洞诱发的，所以及时发现和处理漏洞是安全防范工作的重中之重。国家信息安全漏洞共享平台(CNVD)自成立以来，共收集整理漏洞信息 35032 个。其中，2011 年新增漏洞 5547 个，包括高危漏洞 2164 个(占 39%)、中危漏洞 2529 个(占 45.6%)、低危漏洞 854 个(占 15.4%)。在所收录的上述漏洞中，可用于实施远程网络攻击的漏洞有 4692 个，可用于实施本地攻击的漏洞有 559 个。2011 年，CNVD 共收集、整理了 2164 个高危漏洞，涵盖 Microsoft、IBM、Apple、WordPress、Adobe、Cisco、Mozilla、Novell、Google、Oracle 等厂商的产品。各厂商产品中高危漏洞的分布情况如图 2-1 所示，可以看出，涉及 Apple 产品的高危漏洞最多，占全部高危漏洞的 7.6%。

根据影响对象的类型，漏洞可分为操作系统漏洞、应用程序漏洞、Web 应用漏洞、数据库漏洞、网络设备漏洞(如路由器、交换机等)和安全产品漏洞(如防火墙、入侵检测系统等)。如图 2-2 所示，在 CNVD 2011 年度收集整理的漏洞信息中，操作系统漏洞占 8.8%，应用程序漏洞占 62.5%，Web 应用漏洞占 22.7%，数据库漏洞占 1.1%，网络设备漏洞占 3.7%，安全产品漏洞占 1.2%。

漏洞中最危险的是零日漏洞，一旦针对这些高危漏洞的攻击代码在补丁发布之前被公开或被不法分子知晓，就可能被利用来发动大规模网络攻击。2011 年 CNVD 共收录了 1340 个零日漏洞，主要涉及服务器系统、操作系统、数据库系统以及应用软件等。




图 2-1　2011 年 CNVD 收录高危漏洞的厂商分布

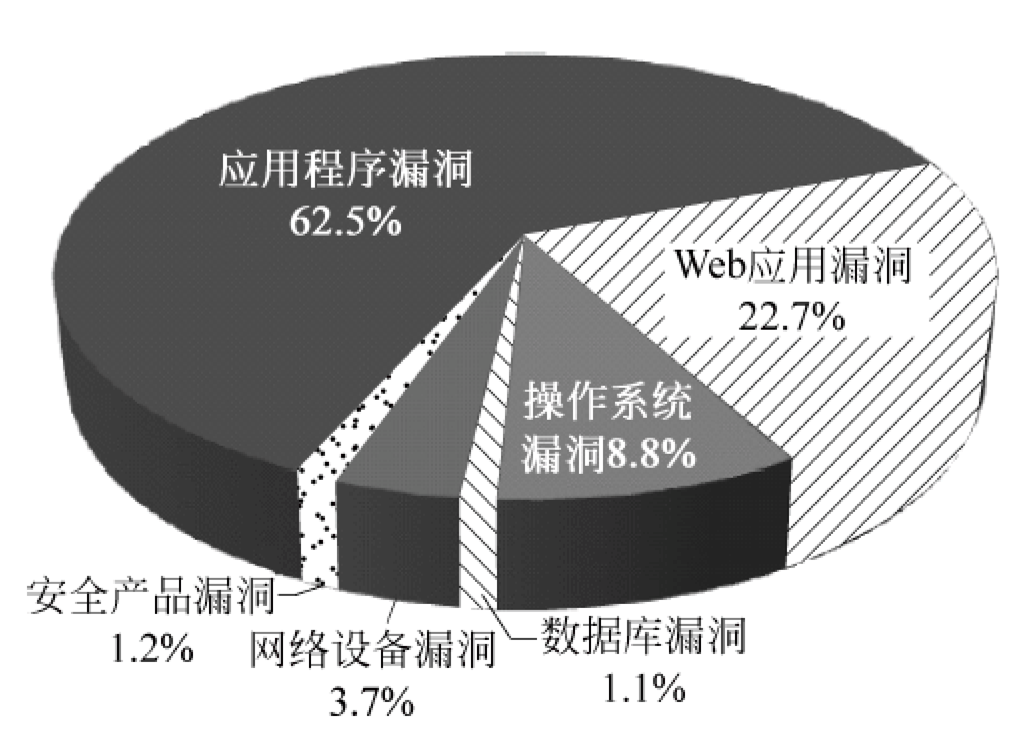


图 2-2　2011 年 CNVD 收录漏洞按影响对象类型分类统计图

2011 年,CNVD 共收录漏洞补丁 3707 个,并为大部分漏洞提供了可参考的解决方案,提醒相关用户注意更新,做好系统加固和安全防范工作。

2012 年 1 月 18 日,Oracle 公司发布的安全更新修复了其多款产品存在的 78 个安全漏洞,61 个安全漏洞可被远程利用,远程或本地攻击者可以进行拒绝服务、SQL 注入和跨站脚本等攻击,进而获得敏感信息,操作数据库,执行任意代码或提升特权。2012 年 2 月,IBM 的多款产品被披露存在多个安全漏洞,远程攻击者可以利用漏洞管理数据和管理员密码、上传文件、以系统权限执行任意代码或使应用程序崩溃。趋势科技对 2012 年第一季度各家公司的系统和软件安全性进行了一次调查,结果发现,苹果所有产品的安全漏洞总数达到 91 个,是业内安全漏洞最多的公司。前十家公司还包括甲骨文,总数为 78 个,谷歌的总数为 73 个,而微软的只有 43 个。据国外媒体报道,Mac OS X 存在一个漏洞,可让黑客 10 秒即可攻破并获取用户的苹果 ID。如果黑客与受影响用户同在一个 Wi-Fi 网络,黑客即可 10 秒获取该用户的苹果 ID。苹果 ID 绑定了用户的 iTunes 和 App Store 的信用卡,因此,泄露了苹果 ID 就等于泄露了信用卡信息。黑客获取苹果 ID 后,可轻易更改密码和邮箱地址。2012 年 4 月,国外研究人员发现 Android 系统存在一个严重漏洞,该漏洞可以被黑客利用发起 DoS 攻击,导致移动设备完全瘫痪。2012 年 5 月,Chrome 19 修复了系统中 20 个安全漏洞,其中 7 个漏洞被 Google 简报称为“出乎意料”的读写缺陷,还有 11 个漏洞是由 Google 的安全小组或委托微软找出的。2012 年 7 月 13 日,雅虎证实大约有 45 万的用户名和密码以及雅虎和其他公司的文件被偷走。一群被称为 D33D 公司的黑客,公布了大约有 453492 个雅虎的用户名和密码。除此之外,他们还公布了包括 Gmail、AOL、Hotmail、Comcast、MSN、SBC Global、Verizon、BellSouth 和 Live.com 用户和密码。黑客是利用软件漏洞,然后使用 SQL 注入的方法盗取了密码。9 月,甲骨文 Java 软件中发现了最新的 0day 漏洞,这一漏洞几乎出现在所有受支持的 Java 版本中,通过此漏洞,黑客可在超过 10 亿台装有 Java 的 Mac 和 PC 机上安装恶意软件与病毒。这一安全漏洞存在于 Java 5、Java 6 和 Java 7 中。2012 年 10 月,Cisco 产品被披露存在多个安全漏洞,攻击者利用漏洞可构建恶意 Web 页,诱使应用程序执行 ActiveX 控件或 Java Applet,执行任意代码;使进程崩溃或者通信中断,发起拒绝服务攻击。

2.2.2 主要端口及漏洞介绍

1. 135 端口及其漏洞

135 端口主要用于使用 RPC(Remote Procedure Call,远程过程调用)协议并提供 DCOM(分布式组件对象模型)服务。通过 RPC,保证在一台计算机上运行的程序可以顺利执行远程计算机上的代码;使用 DCOM 可以通过网络直接通信,能够进行跨协议的多种网络传输。鼎鼎大名的“冲击波”病毒就是利用 RPC 漏洞来攻击计算机的。RPC 本身在处理通过 TCP/IP 的消息交换部分有一个漏洞,该漏洞是由于错误地处理格式不对的消息造成的。该漏洞会影响到 RPC 与 DCOM 之间的一个接口,该接口侦听的端口就是 135。

2. 139 端口及其漏洞

139 端口是为 NetBIOS Session Service 提供的,主要用于提供 Windows 文件和打印机共享以及 UNIX 中的 Samba 服务。在 Windows 中,要在局域网中共享文件,必须使用该服务。开启 139 端口虽然可以提供共享服务,但是常常被攻击者利用,比如使用流光、Super scan 和 X-Scan 等端口扫描软件扫描目标主机的 139 端口。如果发现有漏洞,可以试图获取用户名和密码,因此如果不需要提供文件和打印机共享,建议关闭该端口。

3. 3389 端口

3389 端口是 Windows 操作系统远程桌面的服务端口,可以通过这个端口,用“远程桌面”等连接工具连接到远程的服务器。如果连接上了,输入系统管理员的用户名和密码后,将可以像操作本机一样操作远程服务器,因此远程服务器一般都将这个端口修改数值或者关闭。

2.2.3 扫描器的作用及工作原理

一个端口就是一个潜在的通信通道,也就可以认为是一个入侵通道。对目标计算机端口进行端口扫描,能够得到许多有用的信息。扫描的方法有很多,可以手动进行扫描,也可以用端口扫描软件进行扫描。手动进行扫描时需要熟悉各种命令,还要对命令执行后的输出进行分析。用扫描软件进行扫描时,许多扫描器软件都有分析数据的能力,通过端口扫描可以得到许多有用的信息,从而发现系统的安全漏洞。

扫描器是一种自动检测远程或本地主机安全性弱点的程序,使用扫描器可以不留痕迹地发现远程服务器各种 TCP 端口的分配与提供的服务以及它们的软件版本,从而间接或直接地了解远程主机所存在的安全问题。

黑客在探测目标计算机都开放了哪些端口、提供了哪些服务之前,首先要与目标计算机建立 TCP 连接,这就是扫描的出发点。扫描器向目标计算机的 TCP/IP 服务端口发送探测数据包,并记录目标主机的响应,通过分析响应来判断服务端口是打开还是关闭,就可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地计算机或服务器的流入、流出 IP 数据包来监视本地计算机的运行情况,它仅能对接收到的数据进行分析,帮助用户发现目标计算机的某些内在弱点,而不会提供进入一个系统的详细步骤。

2.2.4 常用端口扫描技术分类

1. TCP Connect Scan(TCP 连接扫描)

TCP 连接扫描是最基本的 TCP 扫描,直接连到目标端口并完成一个完整的 3 次握手

过程(SYN、SYN/ACK 和 ACK)。操作系统提供的 connect()函数完成系统调用,用来与目标计算机端口进行连接。如果端口处于侦听状态,那么 connect()函数就能成功,否则这个端口是无法使用的,也就是没有提供服务。这种扫描技术的最大优点是不需要任何权限,系统中的任何用户都有权利使用这个调用;其次是速度快,通过同时打开多个套接字来加速扫描。其缺点是很容易被发觉,并且被过滤掉。目标计算机的日志文件会显示一连串的连接和连接出错的服务消息,并且能很快地将它关闭。

2. TCP SYN Scan(TCP 同步序列号扫描)

TCP 同步序列号扫描是一种"半开放"式扫描,因为扫描程序不必完成一个完整的 TCP 连接,即扫描主机和目标主机在指定端口建立连接时,只完成前两次握手,在第三步时,扫描主机中断了本次连接,使连接没有完全建立起来。扫描程序发送的是一个 SYN 数据包,好像准备打开一个实际的连接并等待反应一样。这种扫描技术的优点是一般不会在目标计算机上留下记录;缺点是必须要有系统管理员权限,不适合使用多线程技术。

3. TCP FIN Scan(TCP 结束标志扫描)

一些防火墙和包过滤器会对一些特定的端口进行监视,有的程序能检测到 SYN 扫描。FIN 数据包则没有这些麻烦。TCP FIN 扫描的思想是关闭的端口会用适当的 RST 来回复 FIN 数据包,而打开的端口会忽略对 FIN 数据包的回复。但有些系统不管端口打开与否都回复 RST,此时这种扫描方法失效。这种方法在区分 UNIX 和 NT 时,是十分有用的。

4. IP Scan(IP 协议扫描)

IP 协议扫描不直接发送 TCP 协议探测数据包,而是将数据包分成两个较小的 IP 协议段,这样就将一个 TCP 协议头分成几个数据包,使过滤器很难探测到。但有些程序在处理这些小数据包时会有些麻烦。

5. UDP Scan(UDP 协议扫描)

在 UDP 目标端口发送一个 UDP 分组。如果目标端口以"ICMP Port Unreachable(ICMP 端口不可达)"消息作为响应,则该端口是关闭的,否则就是打开的。由于 UDP 是无连接的不可靠协议,因此这种方法的准确性很大程度上取决于与网络及系统资源使用率相关的多个因素。当试图扫描一个大量应用分组过滤功能的设备时,UDP 扫描将是一个非常缓慢的过程。如果在互联网上执行 UDP 扫描,结果是不可靠的。

6. ICMP Echo 扫描

通过 ping 命令判断一个网络上的主机是否开机时非常有效。ping 是最简单的探测手段,用来判断目标是否活动。而且 ping 命令一般在系统内核中实现,不是一个用户进程,因此更加不容易被发现。

2.2.5 常用扫描器介绍

1. 端口扫描器 SuperScan 简介

SuperScan 是一个功能强大的绿色扫描软件,不需要安装即可运行。无论对于黑客还是网络管理员而言,都是必不可少的。它速度很快,探测台湾地区全部回应值小于 200ms 的 IP 段仅用 6 个小时。它可以查看本机 IP 地址和域名,扫描一个 IP 段的所有在线主机以及可探测到的端口号,而且可以保存和导入所有已探测的信息。

SuperScan 的主要功能如下:

（1）IP 和域名相互转换；
（2）检验目标计算机提供的服务类别；
（3）检验一定范围目标计算机是否在线和端口情况；
（4）工具自定义列表检验目标计算机是否在线和端口情况；
（5）自定义要检验的端口，并可以保存为端口列表文件；
（6）检测目标计算机是否有木马。

2. 综合扫描器 X-Scan 简介

X-Scan 是国内最著名的综合扫描器之一，是由“安全焦点”开发的完全免费、不需要安装的绿色软件，界面支持中文和英文两种语言，包括图形界面和命令行方式。对于黑客来讲，X-Scan 是一款非常优秀的扫描器；对于网络管理员来讲，它也不失为一个非常给力的网络安全管理工具。它把扫描报告和“安全焦点”网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便网关测试、修补漏洞等。

X-Scan 采用多线程方式对指定 IP 地址段或单机进行安全漏洞检测，支持插件功能，更提供了图形界面和命令行两种操作方式。扫描内容包括远程服务类型、操作系统类型及版本、标准端口状态及端口信息、SNMP 信息、CGI 漏洞、RPC 漏洞、SSL 漏洞，以及 SQL 服务器、FTP 服务器、SMTP 服务器、POP3 服务器和 NT 服务器弱口令用户，NT 服务器 NetBIOS 信息、注册表信息等。扫描的结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。它和国内其他著名的同类软件相比，扫描更加全面，且无时间、IP 等限制，更适合初学者使用。用它来检查系统的漏洞，可以使系统的安全设置更方便。

2.3 方案设计

方案设计如表 2-1 所示。

表 2-1 方案设计

任务名称	目标系统的探测
任务分解	1. 端口扫描器 SuperScan 的使用 （1）主机名（域名）与 IP 的互相转换 （2）网络工具的使用 （3）端口检测 2. 综合扫描器 X-Scan 的使用 （1）设置扫描参数 （2）利用 X-Scan 扫描目标计算机端口，生成扫描报告 （3）使用 X-Scan 工具进行查询
能力目标	1. 能使用 SuperScan 进行主机名（域名）与 IP 的互相转换 2. 能使用 SuperScan 检测目标计算机是否在线，并判断网络状况 3. 能使用 SuperScan 对主机和服务进行扫描设置 4. 能使用 SuperScan 检测目标计算机提供的服务 5. 能使用 SuperScan 检测目标计算机的所有端口 6. 能使用 SuperScan 扫描目标计算机的特定端口 7. 能对 X-Scan 设置扫描参数 8. 能使用 X-Scan 扫描目标计算机端口，生成扫描报告 9. 能使用 X-Scan 工具查询物理地址

续表

知识目标	1. 了解漏洞的分类 2. 熟悉扫描器的作用 3. 了解扫描器的工作原理 4. 了解常用端口扫描技术分类 5. 了解常用的网络探测方法 6. 了解常用扫描器的功能及优缺点
素质目标	1. 掌握网络安全行业的基本情况 2. 培养良好的职业道德 3. 具有良好的团队协作和沟通交流能力 4. 培养创新能力 5. 树立较强的安全、节约、环保意识

24 任务实施

2.4.1 任务1：端口扫描器 SuperScan 的使用

1. 任务目标

使用 SuperScan 进行端口扫描，检验 IP 是否在线，实现 IP 和域名互相转换，检验目标计算机提供的服务类别，检验一定范围的目标计算机是否在线和端口情况。

2. 工作任务

(1) 主机名(域名)与 IP 的互相转换；

(2) 网络工具的使用；

(3) 端口检测。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机，通过网络相连。

(2) 软件工具：SuperScan。

4. 实施过程

如果 SuperScan 的版本号是 4.0，下面根据具体功能来介绍使用方法。

(1) 主机名(域名)与 IP 互相转换

这个功能的作用就是根据域名取得 IP，比如根据 www.qq.com 得到 IP；或者根据 IP 123.129.194.144 取得域名。

启动 SuperScan 4.0 后，在其主界面中切换到“扫描”选项卡。在“IP 地址”区域的“主机名/IP”文本框中输入要转换的主机名或者 IP 地址，然后单击后面的转换按钮即可，如图 2-3 所示。

(2) 网络工具的使用

SuperScan 提供了查找主机名/IP、ping、ICMP 跟踪和路由跟踪 4 种工具，其使用方法如下所示。

① 查找主机名/IP：在“工具”选项卡中的“主机名/IP/URL”文本框内输入主机名、IP



图 2-3 “扫描”选项卡

或者 URL，然后单击“查找主机名/IP”按钮，如图 2-4 所示。

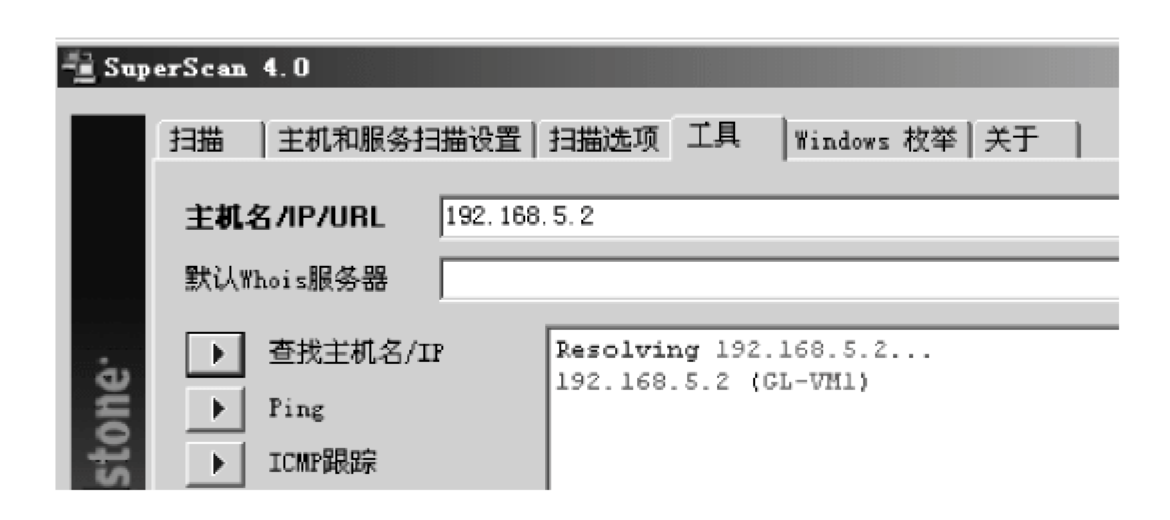


图 2-4 查找主机名/IP

② ping 的主要目的在于检测目标计算机是否在线和通过反应时间判断网络状况。使用“Ping”按钮，如果能 ping 通，说明这两台计算机是可以进行数据传输的，如图 2-5 所示。

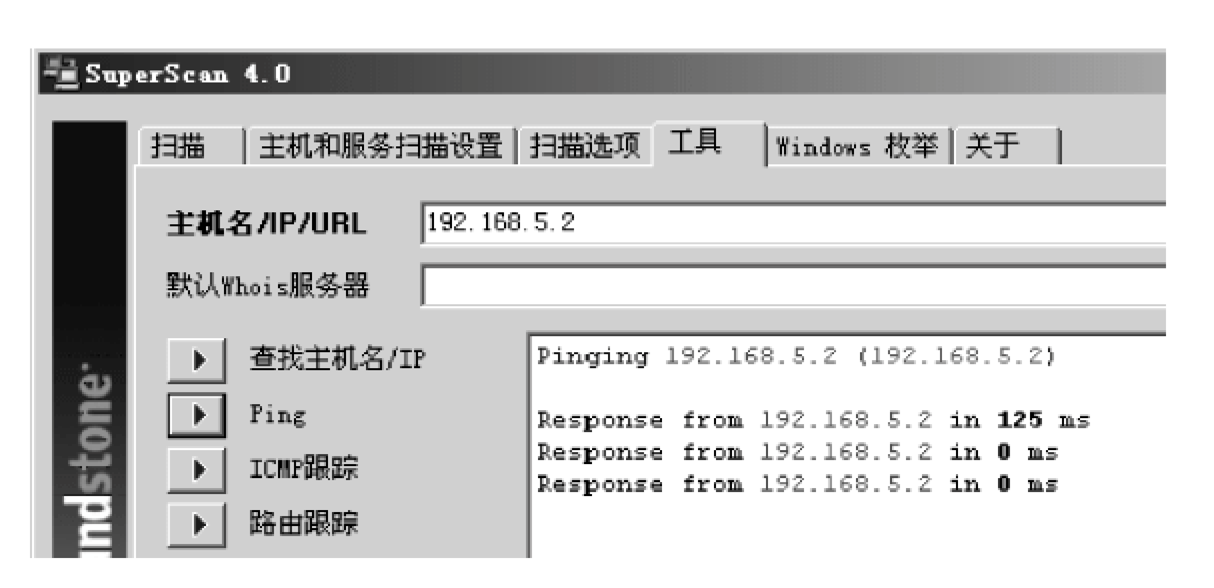


图 2-5 使用“Ping”按钮

③ 路由跟踪：单击“路由跟踪”按钮即可对远程主机进行路由跟踪，如图 2-6 所示。



图 2-6 路由跟踪

(3) 端口检测

① 主机和服务扫描设置：切换到“主机和服务扫描设置”选项卡，对主机和服务扫描设

置，如图 2-7 所示。

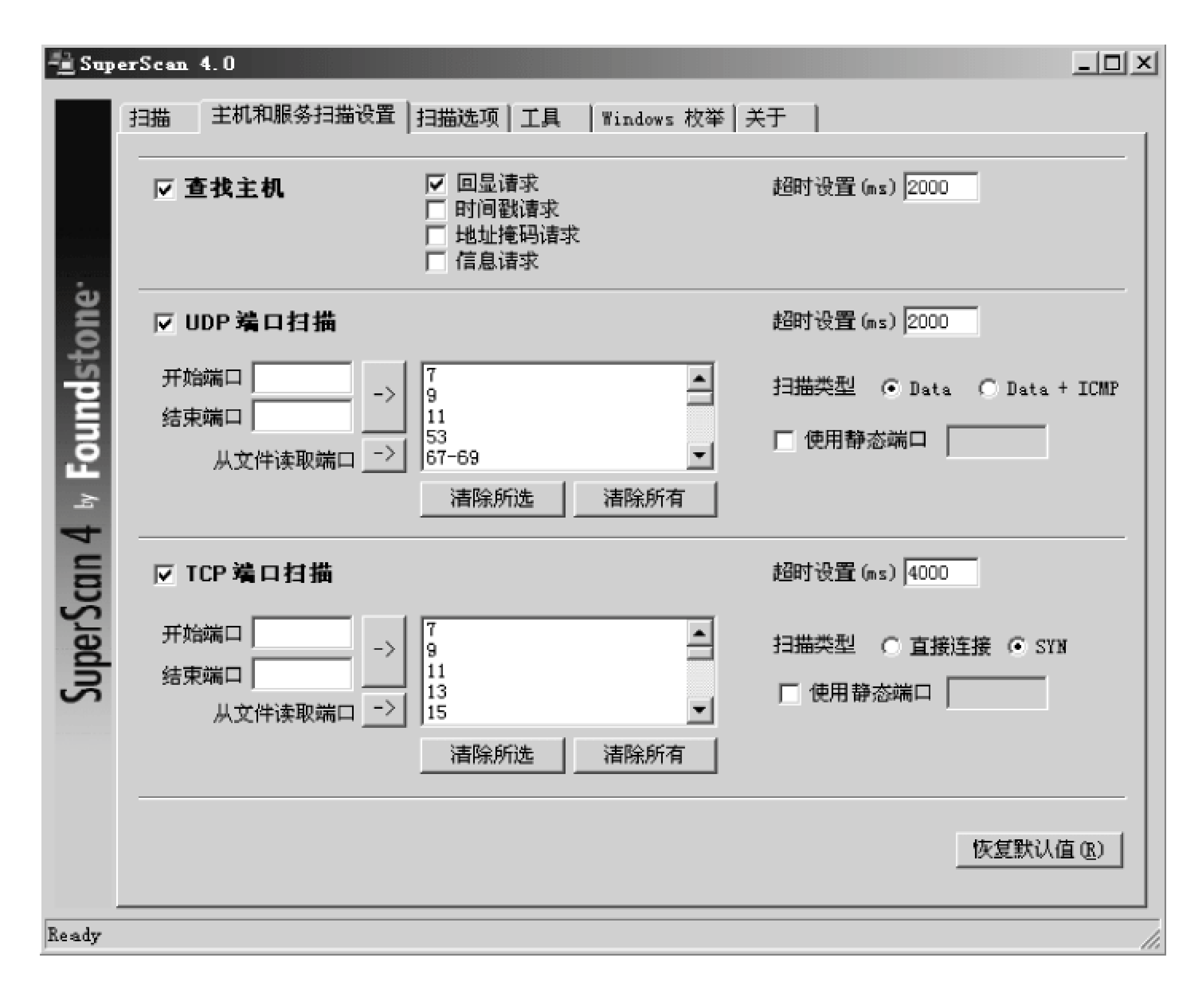


图 2-7　“主机和服务扫描设置”选项卡

② 切换到“扫描选项”选项卡，对基本扫描做一些设置，如图 2-8 所示。



图 2-8　“扫描选项”选项卡

③ 设置完毕，返回“扫描”选项卡，单击“开始”按钮即可开始扫描端口，扫描的相应信息会在窗口中显示出来。

如果 SuperScan 的版本号是 3.0，下面根据具体功能来介绍使用方法。

（1）主机名（域名）与 IP 互相转换

有两种方法来实现此功能。

① 通过“Hostname Lookup”来实现。在“Hostname Lookup”的输入框输入需要转换的域名或 IP，然后单击“Lookup”按钮取得结果，如图 2-9 所示。



图 2-9　主机名(域名)和 IP 互相转换

如果需要取得本地计算机的 IP，单击“Me”按钮；同时，可以取得本地计算机的 IP 设置情况，单击“Interfaces”按钮即可，如图 2-10 所示。



图 2-10　本地 IP 设置情况

② 通过“Extract From File”实现。这个功能是指通过一个域名列表来将域名转换为相应的 IP 地址，方法是：选择“Extract From File”，然后单击向右箭头按钮，选择域名列表进行转换。

(2) ping 功能的使用

在 IP 的“Start”填入起始 IP，在“Stop”填入结束 IP，然后在“Scan type”中选择“Ping only”，单击“Start”按钮就可以检测了，如图 2-11 所示。

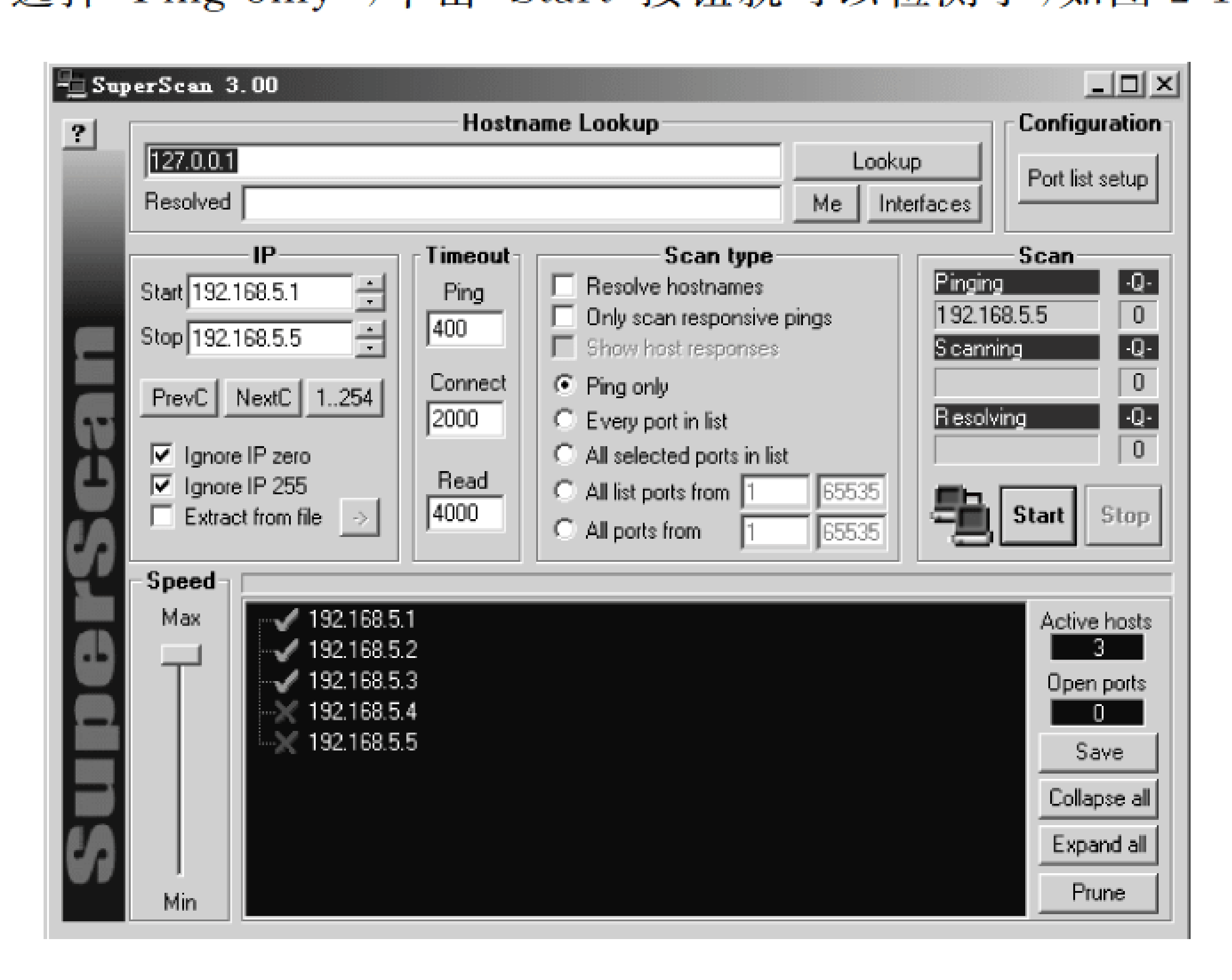


图 2-11　SuperScan 的 ping 功能

在以上设置中，选择“Ignore IP zero”可以屏蔽所有以 0 结尾的 IP；选择“Ignore IP 255”可以屏蔽所有以 255 结尾的 IP。

(3) 端口检测

端口检测可以取得目标计算机提供的服务，同时，可以检测目标计算机是否有木马。

① 检测目标计算机的所有端口。如果检测的时候没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测。一般不提倡这种检测，首先，因为它会对目标主机的正常运行造成一定的影响，也会引起目标计算机的警觉；其次，扫描的时间很长；最后，它浪费带宽资源，对网络正常运行造成影响。

在 IP 输入起始 IP 和结束 IP，然后在“Scan type”选择最后一项“All ports from 1 to 65535”。如果需要返回计算机的主机名，可以选择“Resolve hostnames”，单击“Start”按钮开始检测。图 2-12 所示是对一台目标计算机所有端口进行扫描的结果。扫描完成以后，按“Expand all”展开，可以看到扫描的结果。第一行是目标计算机的 IP 和主机名，从第二行开始是扫描的计算机的活动端口号和对该端口的解释。“Active hosts”显示扫描到的活动主机数量，这里只扫描到了一台，为“1”；“Open ports”显示目标计算机打开的端口数，这里是“7”。

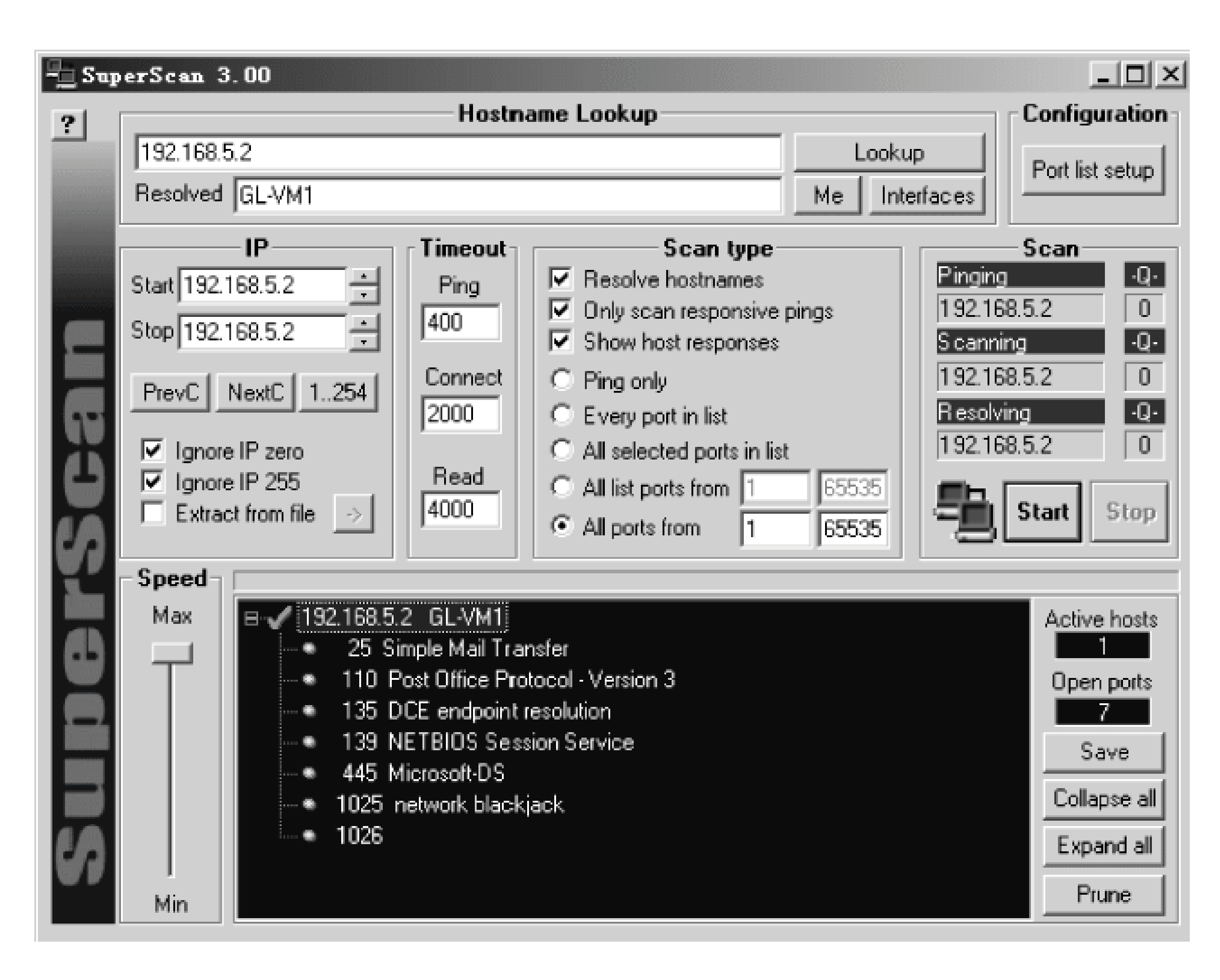


图 2-12　端口检测

② 扫描目标计算机的特定端口(自定义端口)。其实大多数时候并不需要检测所有端口，只要检测有限的几个端口就可以了。因为检测的目的只是为了得到目标计算机提供的服务和使用的软件，所以可以根据个人目的的不同来检测不同的端口，一般只要检测 80(Web 服务)、21(FTP 服务)和 23(Telnet 服务)就可以了，即使是攻击，也不会有太多的端口检测。

单击“Port list setup”按钮，出现端口设置界面，如图 2-13 所示。在端口设置界面中，双击需要扫描的端口，其前面会有一个绿色的对钩。选择的时候，注意对话框左边的“Change/add/delete port info”和“Helper apps in right-click menu”是对此端口的详细说明和所使用的程序。在此选择 21、23 和 80 3 个端口，然后单击“Save”按钮保存选择的端口为端口列表。单击“OK”按钮回到主界面。在“Scan type”区域选择“All selected ports in list”，然后单击“Start”按钮开始检测。

使用自定义端口的方式时需要注意以下几点：选择端口时可以详细了解端口信息；选择的端口可以自己取名保存，有利于再次使用；可以根据工具要求有的放矢地检测目标端口，节省时间和资源；根据一些特定端口，可以检测目标计算机是否被攻击者利用、种植木马或者启动不应该启动的服务。

③ 检测目标计算机是否被种植木马。现在有很多木马清除工具，如果只是检测木马，可以用 SuperScan 来实现，因为所有木马都必须打开一定的端口，只要检测这些特定的端口，就可以知道计算机是否被种植木马。在主界面选择“Port list setup”，将出现端口设置界面，然后单击“Port list file”的下拉列表框选择“trojans. lst”端口列表文件，如图 2-14 所

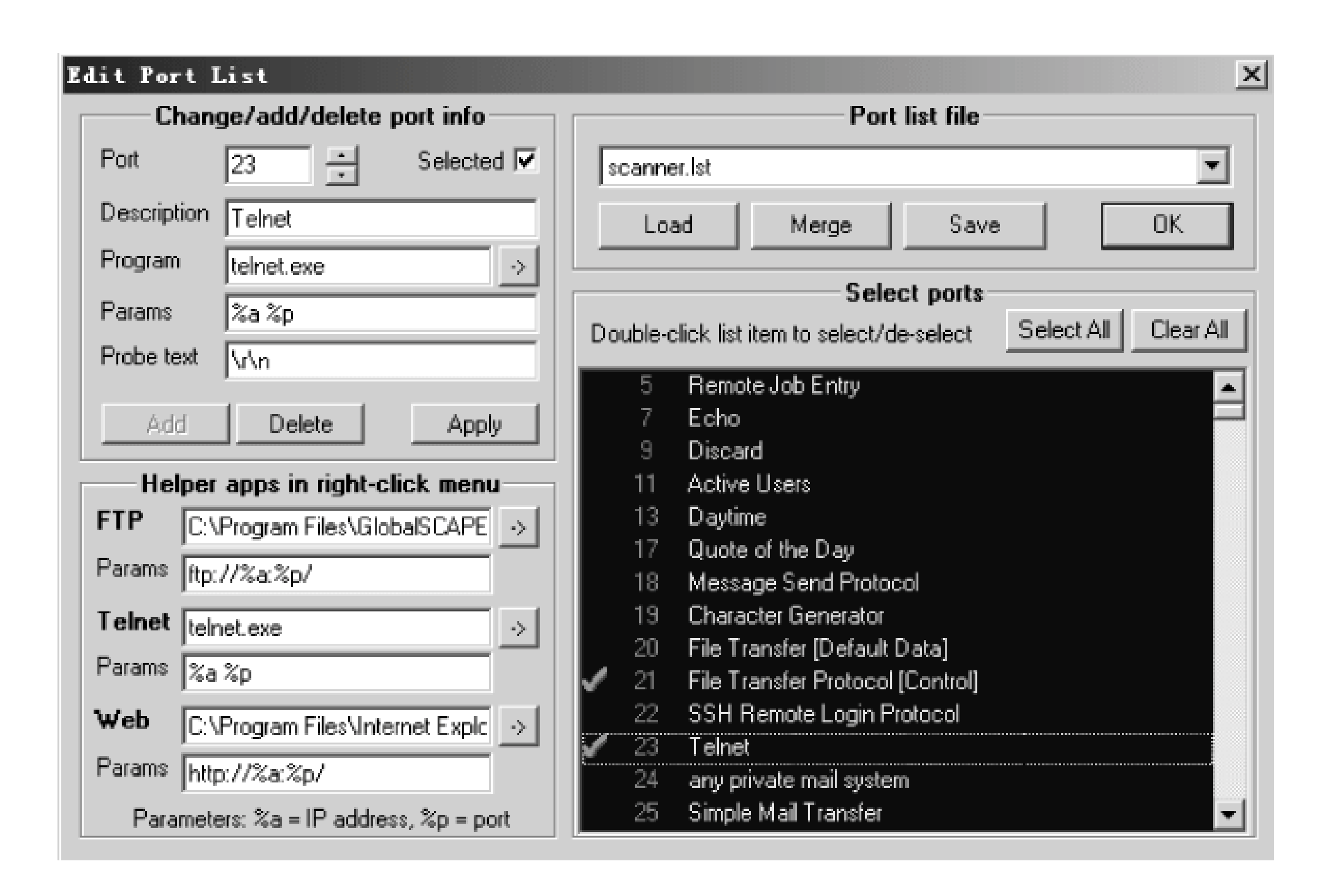


图 2-13 扫描目标计算机的特定端口

示。这个文件是软件自带的，提供了常见的木马端口，可以使用这个端口列表来检测目标计算机是否被种植木马。需要注意的是，有必要时常注意最新出现的木马和它们使用的端口，随时更新木马端口列表。

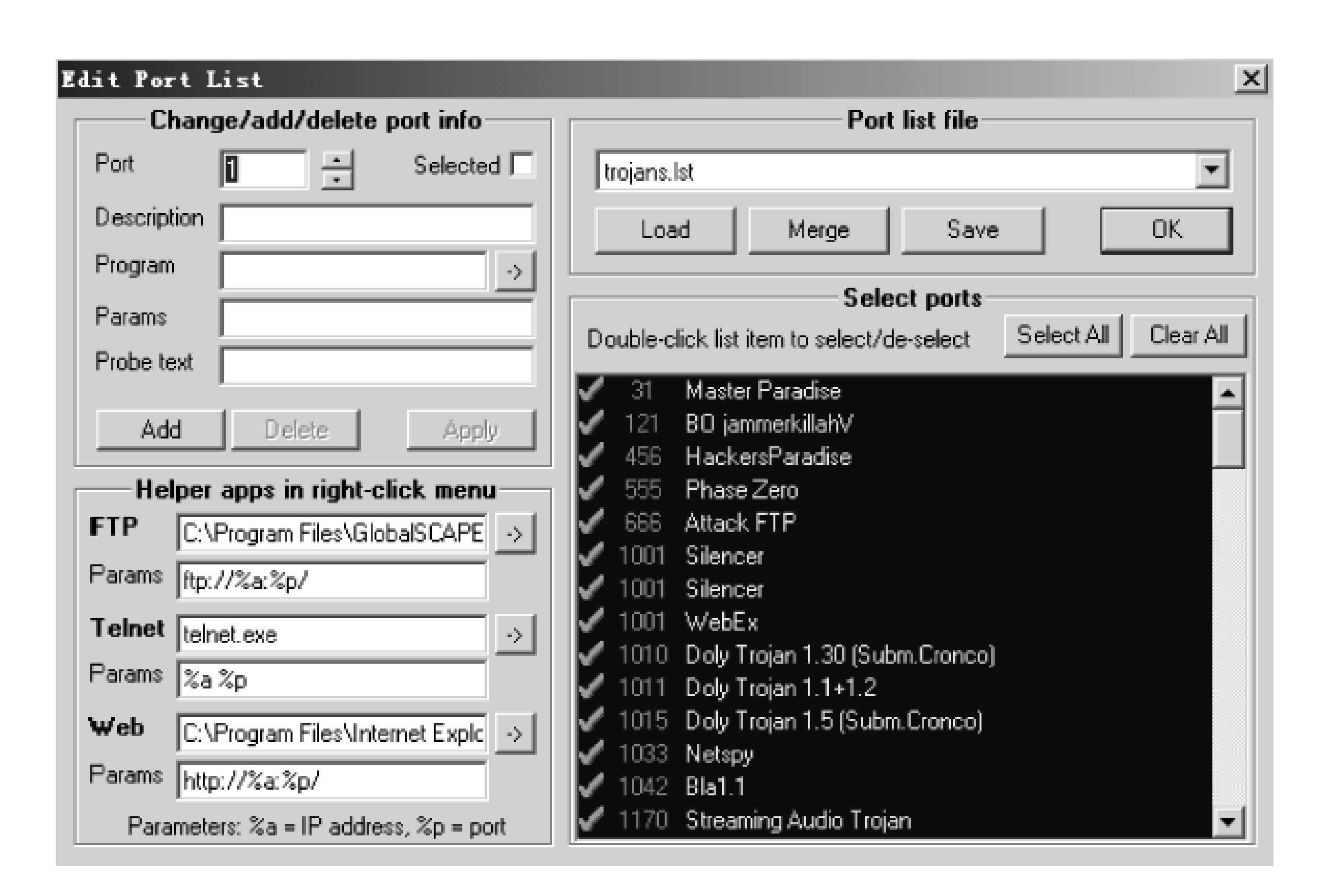


图 2-14 检测目标计算机是否被种植木马

2.4.2 任务 2：综合扫描器 X-Scan 的使用

1. 任务目标

使用 X-Scan 对目标计算机的端口状态、操作系统相关信息进行扫描。

2. 工作任务

(1) 设置扫描参数；

(2) 利用 X-Scan 扫描目标计算机端口，生成扫描报告；

(3) 使用 X-Scan 工具进行查询。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机，通过网络相连。

（2）软件工具：X-Scan。

4. 实施过程

（1）设置扫描参数

对 X-Scan 软件设置扫描参数的具体操作如下：

① 双击 X-Scan 应用程序图标启动该软件，然后选择“设置”→“扫描参数”菜单项，如图 2-15 所示。

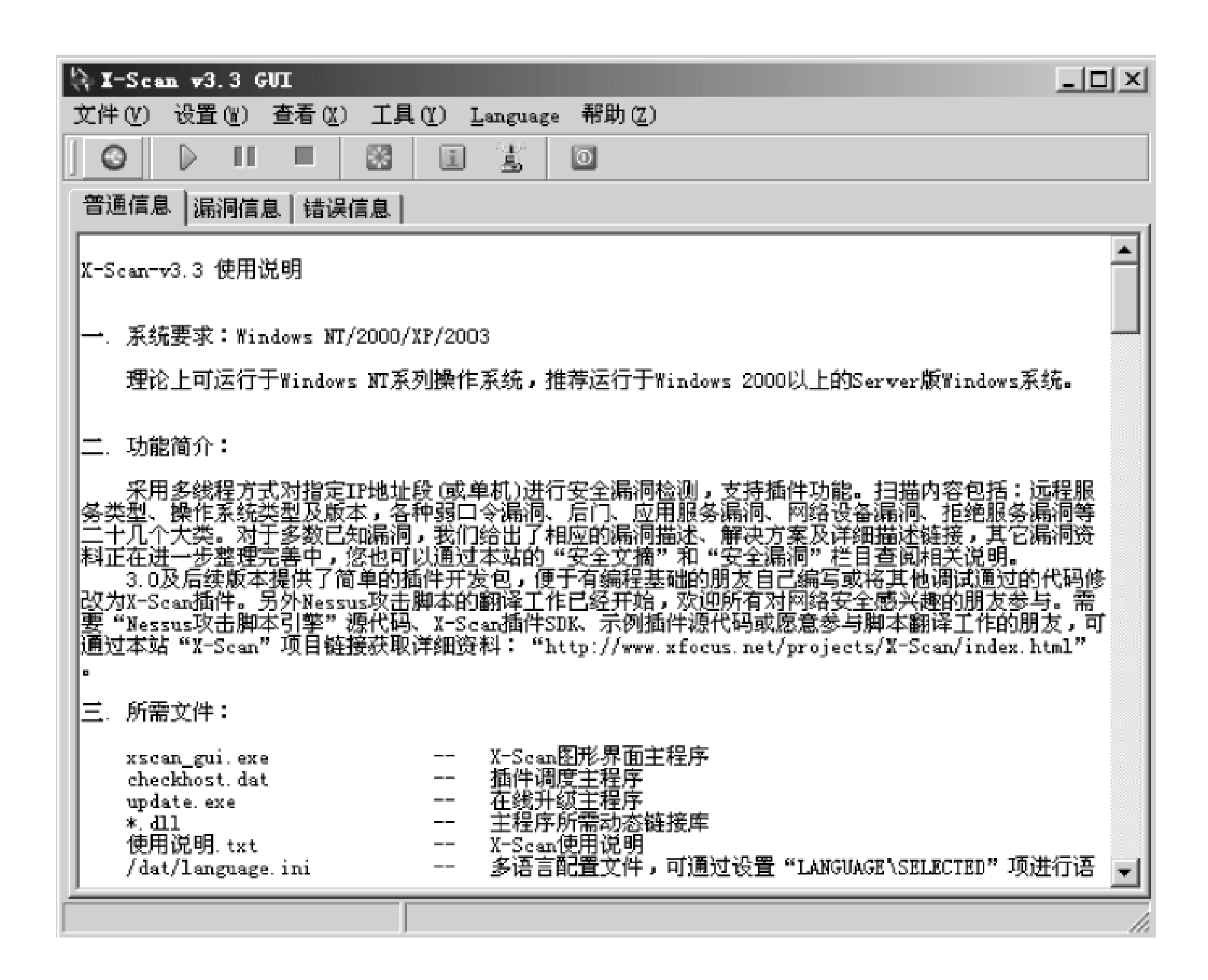


图 2-15　X-Scan 主窗口

② 在弹出的“扫描参数”对话框左侧的区域中选择“检测范围”选项，然后单击右侧的“指定 IP 范围”文本框后的“示例”按钮，在“示例”窗口中查看有效示例格式，如图 2-16 所示。

③ 单击“确定”按钮，然后在右侧的“指定 IP 范围”文本框中根据示例格式输入 IP 地址段。这里输入“192.168.5.1-192.168.5.2”，如图 2-17 所示。



图 2-16　“示例”窗口

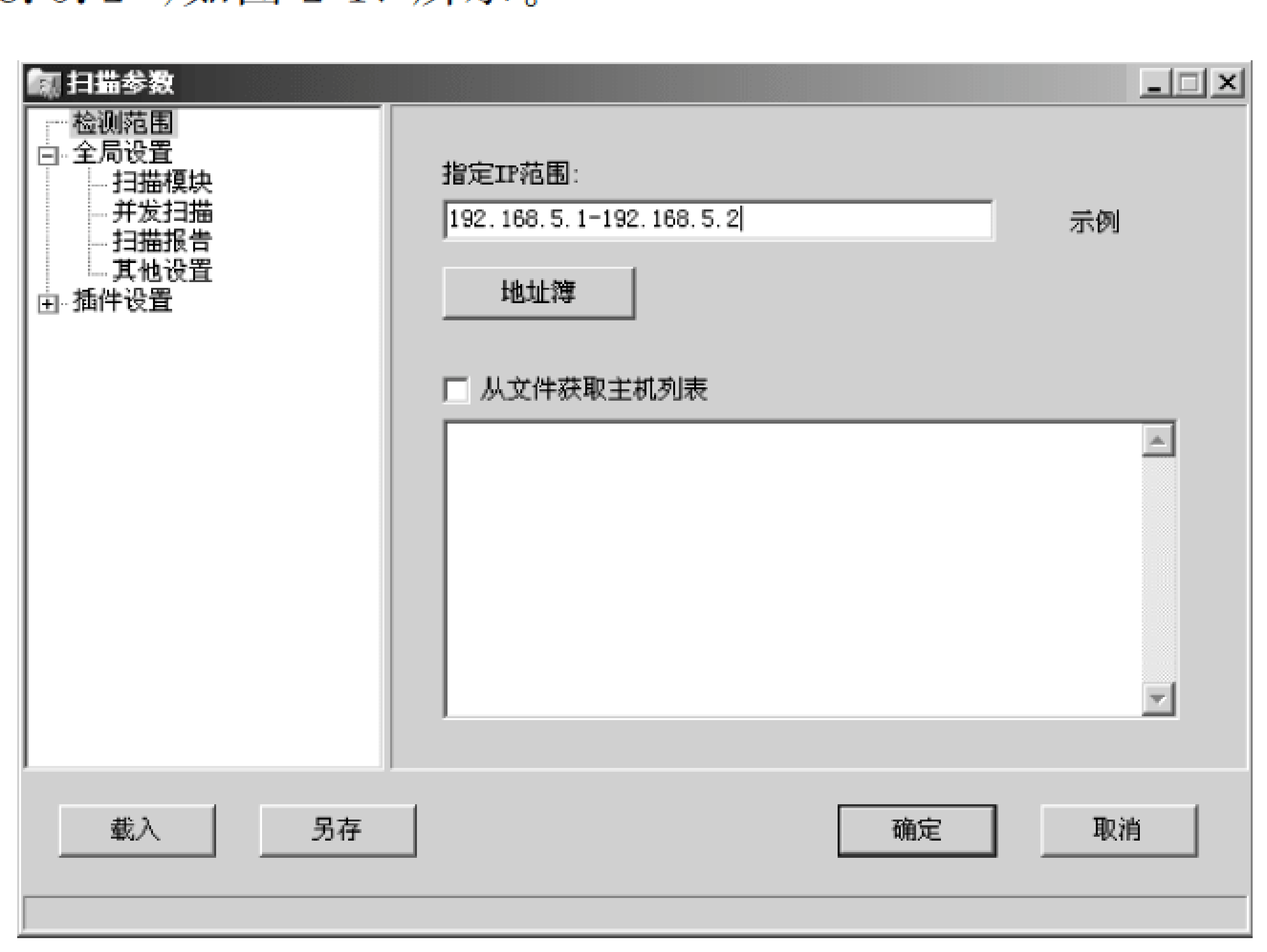


图 2-17　指定 IP 范围

④ 在对话框左侧区域中展开"全局设置"项,然后选择"扫描模块"选项;在中间列表框中选中扫描时需要使用的模块前的复选框,如图 2-18 所示。



图 2-18 选择"扫描模块"选项

⑤ 选择"并发扫描"选项,在其中的"最大并发主机数量"文本框中输入"10",在"最大并发线程数量"文本框中输入"100",如图 2-19 所示。



图 2-19 指定"最大并发主机数量"

⑥ 选择"扫描报告"选项,设置扫描报告文件的名称和类型,如图 2-20 所示。

⑦ 选择"其他设置"选项,然后选中"跳过没有响应的主机"单选按钮,再选中"跳过没有检测到开放端口的主机"和"使用 NMAP 判断远程操作系统"复选框,并单击"确定"按钮,如图 2-21 所示。

⑧ 展开"插件设置"项,然后选择"端口相关设置"选项,设置待检测的端口和检测方式,并单击"确定"按钮,如图 2-22 所示。



图 2-20　设置扫描报告文件的名称和类型

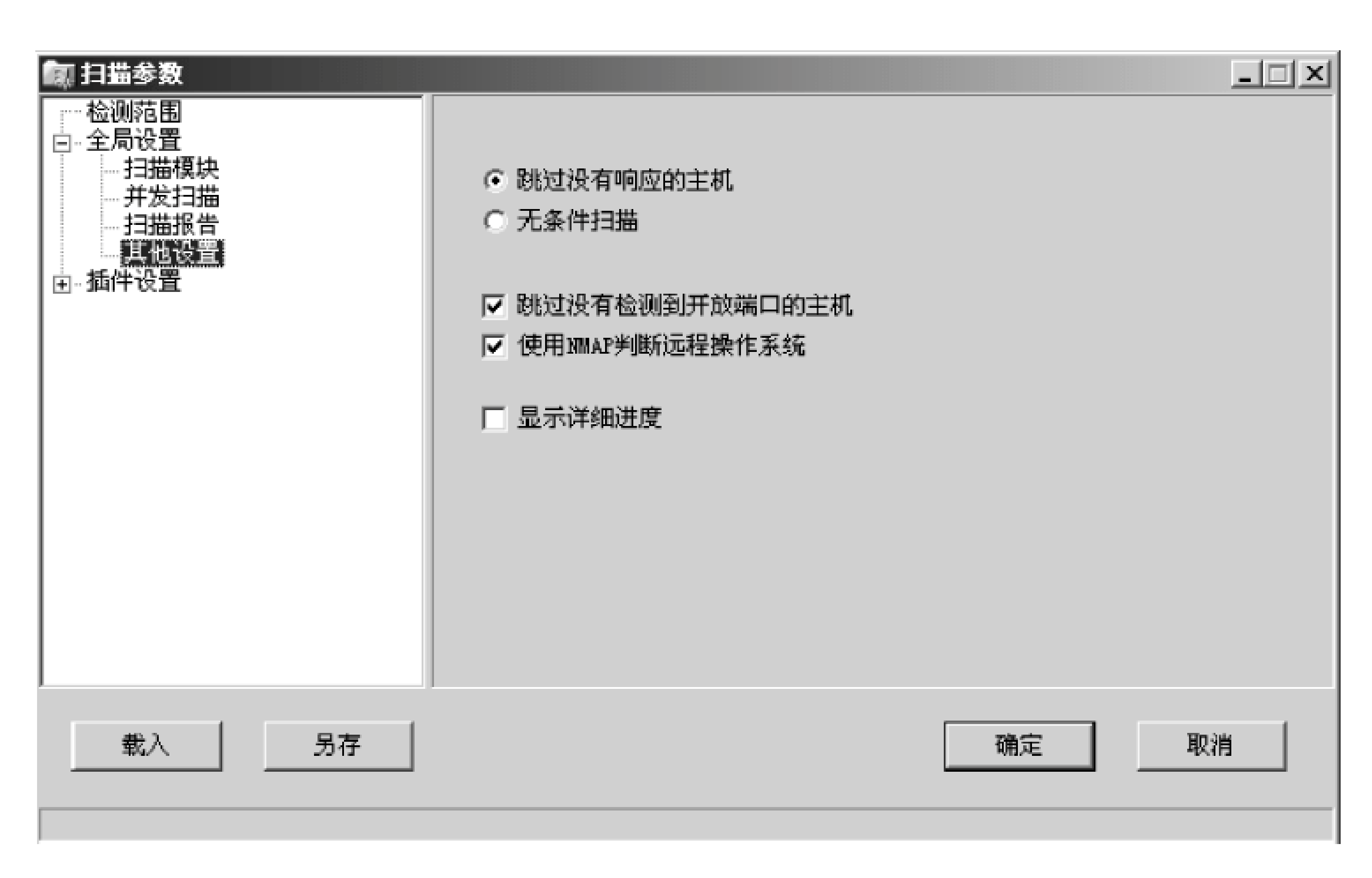


图 2-21　“其他设置”选项设置

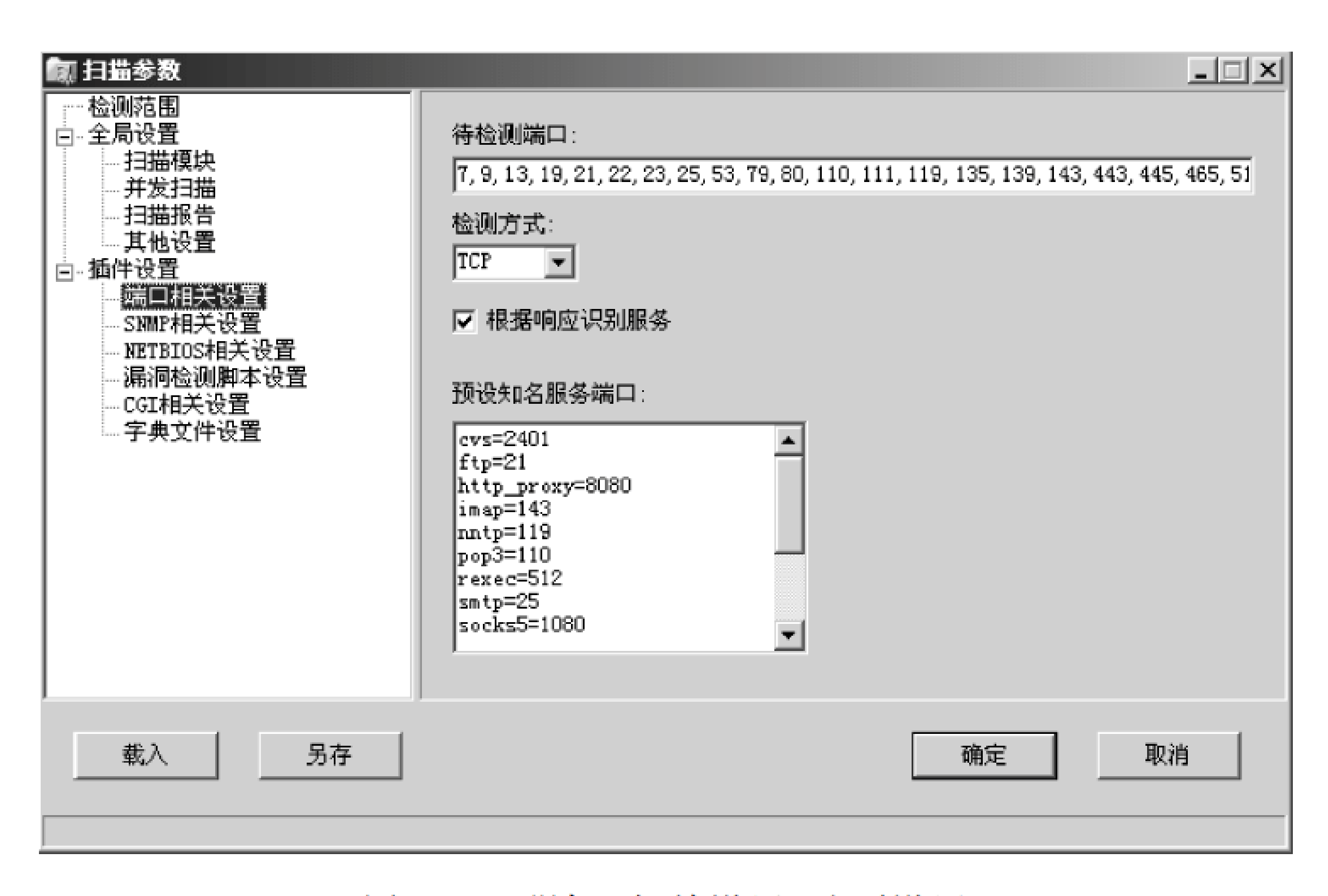


图 2-22　“端口相关设置”选项设置

⑨ 选择“SNMP相关设置”选项，设置在扫描时获取简单网络管理协议的相关信息，如图2-23所示。

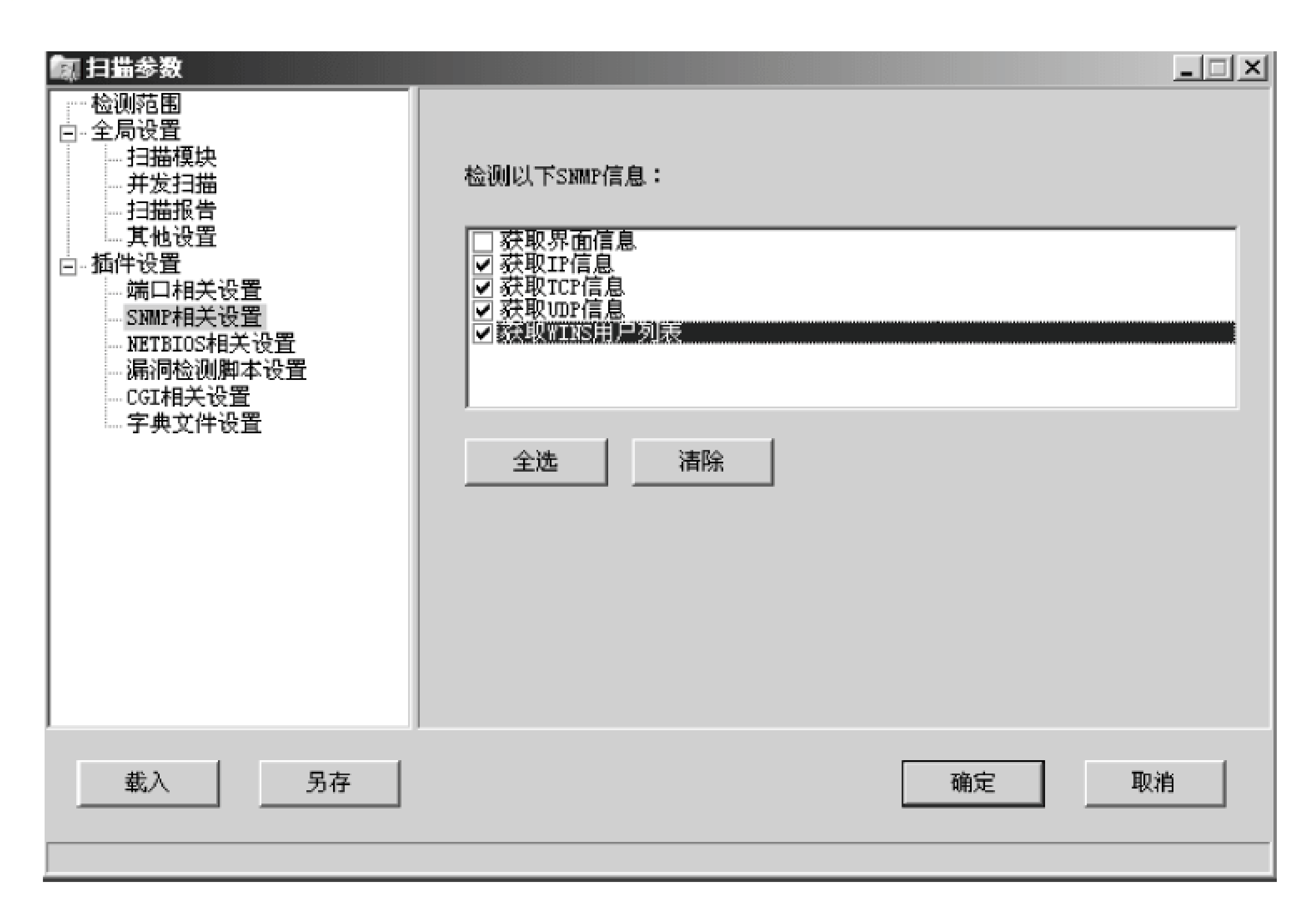


图2-23 “SNMP相关设置”选项设置

⑩ 选择“NETBIOS相关设置”选项，设置需要检测的NETBIOS的相关信息，如图2-24所示。



图2-24 “NETBIOS相关设置”选项设置

⑪ 选择“漏洞检测脚本设置”选项，选择要使用的脚本，设置脚本运行超时时间和网络读取超时时间，如图2-25所示。

⑫ 选择“CGI相关设置”选项，对通用网关接口进行设置；选中“用‘HEAD’替换‘GET’”单选按钮，如图2-26所示。

⑬ 选择“字典文件设置”选项，再在右侧的字典列表框中选择需要的字典文件，然后单击“确定”按钮关闭“扫描参数”对话框，如图2-27所示。



图 2-25　“漏洞检测脚本设置”选项设置



图 2-26　“CGI 相关设置”选项设置



图 2-27　“字典文件设置”选项设置

(2) 使用 X-Scan 扫描目标计算机端口，生成扫描报告

使用 X-Scan 扫描目标计算机的具体操作如下：

① 在 X-Scan 操作界面，单击“开始扫描”按钮，按设置对目标计算机进行扫描，如图 2-28 所示。



图 2-28　X-Scan 操作界面

② 扫描完成后，X-Scan 将把扫描结果保存为一个 HTML 文件并打开，从中可以查看目标计算机的信息，如图 2-29 所示。

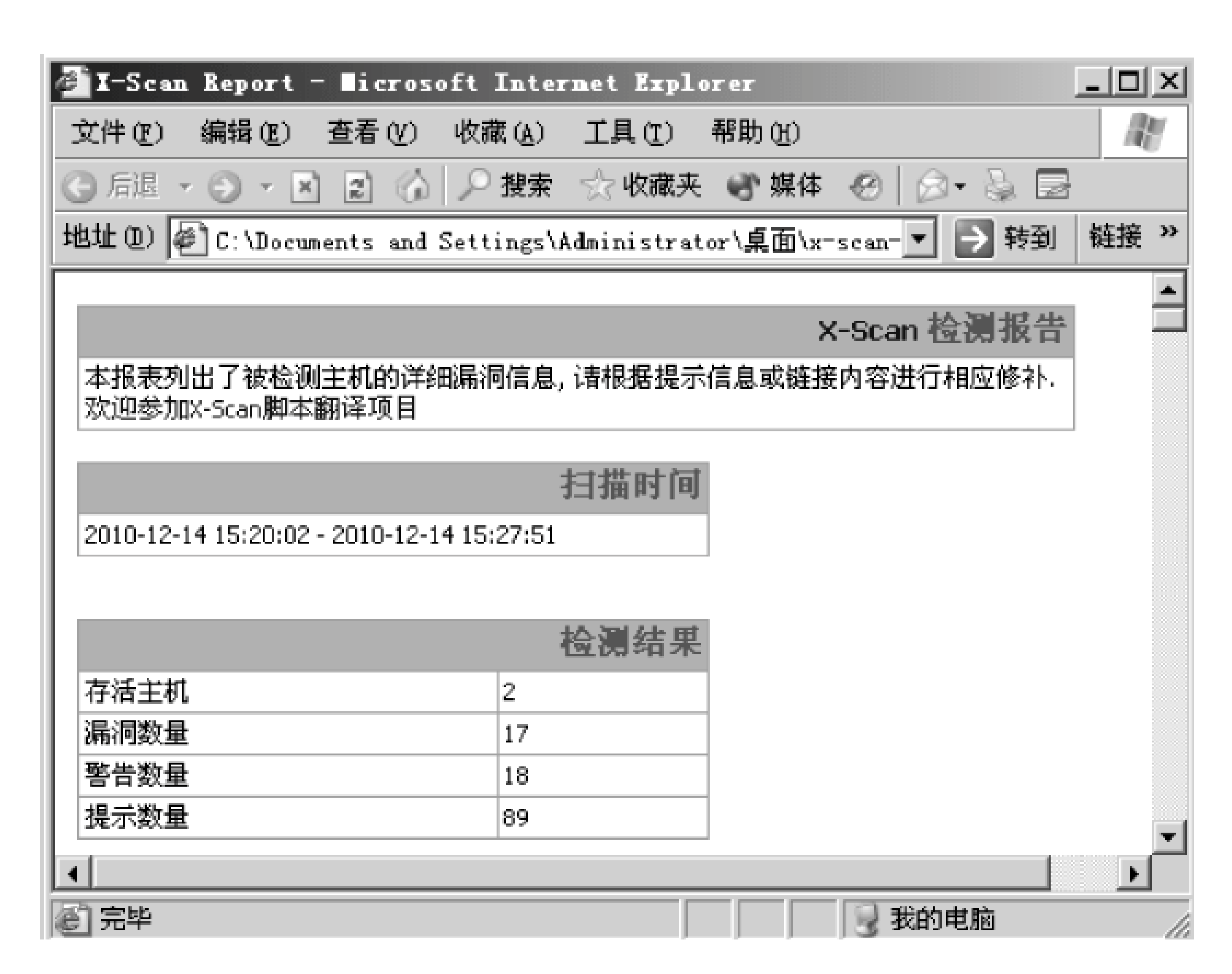


图 2-29　扫描结果

(3) 使用 X-Scan 工具查询物理地址

使用目标主机的 IP 地址或主机名可以查询到该 IP 地址主机的其他一些基本信息，具体操作如下：

① 在 X-Scan 主界面的菜单栏中，选择“工具”→“物理地址查询”菜单项。

② 在“工具”对话框的“物理地址查询”选项卡中输入 IP 地址或者主机名，可以查询到该 IP 地址主机的其他一些基本信息，如图 2-30 所示。



图 2-30　“物理地址查询”选项卡

25　常见问题解答

1．扫描的作用是什么？

答：通过扫描结果，可以看到在计算机上开放了哪些端口、启动了哪些服务。如果看到一些显示为未知的或看上去可疑的服务，可以记下端口号，然后通过谷歌或百度等搜索引擎进行搜索，看看这个端口具体是干什么的。

2．如何关闭端口？

答：在计算机上，有些开放的端口可能是应用程序所需要的，但如果有开放端口是不必要的，例如有些服务是以前有用而现在已经不用的，那么停止这些服务，从而关闭相应的开放端口，减少安全隐患。从控制面板的管理工具中打开“服务”管理窗口，找到需要关闭的服务，将其启动类型改为“禁用”，即可停止该项服务。

3．如何屏蔽 139 端口？

答：139 端口可以通过禁用 NetBIOS 来屏蔽，方法：在“网络连接”窗口中右击“本地连接”图标，在弹出的“本地连接属性”对话框中选择“Internet 协议(TCP/IP)”选项；然后单击“属性”按钮，打开“Internet 协议(TCP/IP)属性”对话框，在该对话框中单击“高级”按钮，在“高级 TCP/IP 设置”对话框中选择“WINS”选项卡，再选择“禁用 TCP/IP 上的 NetBIOS”单选按钮；最后依次单击“确定”按钮。

4．X-Scan 自带的字典存放在哪里？它的大小与扫描时间有何关系？

答：X-Scan 自带的字典存放在 dat 文件夹中，用户可以对这些文件进行修改。扫描时，选择的字典文件越大，扫描的时间越长。

5．如何防止黑客的扫描？

答：要防止黑客的扫描，需要安装防病毒软件及防火墙，并及时升级病毒库，防止有破

坏性程序的注入;使用最新版本的浏览器软件、电子邮件软件及其他程序;不要轻易打开来历不明的电子邮件或软件,因为它可能包含后门程序或其他有害程序;在使用 QQ、MSN 等聊天工具时,不轻易同意陌生人加自己为好友;使用可以对 Cookie 进行控制的安全程序,因为 Cookie 有时会泄露用户的一些个人隐私;经常查找自己计算机中存在的漏洞,并下载安装漏洞补丁,防止黑客利用漏洞进行攻击。

26 过关练习

一、选择题

1. (　　)类型的软件能够阻止外部主机对本地计算机的端口扫描。
   A. 杀病毒软件　　B. 个人防火墙
   C. 基于 TCP/IP 的检查攻击,例如 netstat　　D. 加密软件
2. 传输安全电子邮件的协议 PGP 属于(　　)。
   A. 物理层　　B. 传输层　　C. 网络层　　D. 应用层
3. 关于网络安全,以下说法正确的是(　　)。
   A. 使用无线传输可以防御网络监听
   B. 木马是一种蠕虫病毒
   C. 使用防火墙可以有效地防御病毒
   D. "冲击波"病毒利用 Windows 的 RPC 漏洞进行传播
4. 许多黑客利用软件实现中的缓冲区溢出漏洞进行攻击。对于这一威胁,最可靠的解决方案是(　　)。
   A. 安装防火墙　　B. 安装用户认证系统
   C. 安装相关的系统补丁软件　　D. 安装防病毒软件

二、简答题

1. 常用的扫描器有哪些?
2. 端口扫描分为哪几类?扫描器的工作原理是什么?

工作任务三

口令破解

3.1 用户需求与分析

如果黑客已经找到目标主机，在攻击过程中一般都会对计算机系统的登录账号和密码进行破解，以便使用这些登录账号和密码进入目标主机系统，从而控制目标主机。

3.2 预备知识

3.2.1 口令破解的意义

为了安全，现在几乎所有的系统都通过访问控制来保护自己的数据。访问控制最常用的方法就是口令保护，又称为密码保护。口令应该说是用户最重要的一道防护门，如果密码破解了，用户的信息将很容易被窃取，因此口令破解也是黑客入侵系统比较常用的方法。或者，当公司的某个系统管理员离开企业而其他人都不知道该管理员账号的口令时，企业可能会聘请专业技术人员来破解管理员口令。

3.2.2 获取用户密码的方法

一般入侵者常常通过下面几种方法获取用户的密码口令：暴力破解、sniffer 密码嗅探、木马程序或键盘记录程序等。有关系统用户账号密码口令的暴力破解主要是基于密码匹配的破解方法，最基本的方法有两个：穷举法和字典法。穷举法是效率最低的方法，是将字符或数字按照穷举的规则生成口令字符串，进行遍历尝试。在口令稍微复杂的情况下，穷举法的破解速度很慢。字典法相对来说效率较高，指用口令字典中事先定义的常用字符去尝试匹配口令。口令字典是一个很大的文本文件，可以自己编辑或者由字典工具生成，里面包含了单词或者数字的组合。如果密码是一个单词或者是简单的数字组合，破解者可以很轻易地破解密码。

常用的密码破解工具有很多，通过使用工具，可以了解口令的安全性，下面介绍两种最常见的工具软件。随着网络黑客攻击技术的增强和提高，很多口令都可以被攻击和破译，这就要求用户提高对口令安全的认识。

1. 流光扫描器简介

流光扫描器是黑客必备的扫描器之一，它除了可以扫描系统安全漏洞、弱口令之外，还集成了常用的入侵字典，如字典工具、NT/IIS 工具等，并且独创了能够控制“肉鸡”进行扫描的流量 sensor 工具和为“肉鸡”安装服务的“种植者”工具。流光扫描器的功能较多，操作

较复杂，其功能还在进一步扩充。流光扫描器的作者为了防止该工具用于非法目的，非注册版对其使用功能进行了限制，且不能扫描国内的 IP 地址。

2. SMBcrack 工具软件简介

SMBcrack 是基于 Windows 操作系统的口令破解工具，是小榕软件为流光扫描器开发的测试原型。它与以往的 SMB(共享)暴力破解工具不同，没有采用系统的 API，而是使用了 SMB 的协议。因为 Windows 可以在同一会话内进行多次密码探测，所以用 SMBcrack 可以破解操作系统的口令。

3.3 方案设计

方案设计如表 3-1 所示。

表 3-1 方案设计

任务名称	口令破解
任务分解	1. 使用流光扫描器探测目标主机 (1) 使用流光扫描器探测目标主机 (2) 使用流光扫描器制作黑客字典 2. 使用 SMBcrack 进行口令破解
能力目标	1. 能使用流光扫描器探测目标主机 2. 能使用流光扫描器制作黑客字典 3. 能使用 SMBcrack 工具软件进行口令破解
知识目标	1. 了解口令破解的意义 2. 熟悉获取用户密码的方法 3. 了解流光扫描器的作用 4. 了解 SMBcrack 工具软件的作用
素质目标	1. 培养良好的职业道德 2. 具有良好的团队协作和沟通交流能力 3. 掌握网络安全行业的基本情况 4. 培养创新能力 5. 树立较强的安全、节约、环保意识

3.4 任务实施

3.4.1 任务 1：使用流光扫描器探测目标主机

1. 任务目标

通过流光扫描器的使用，了解账户的安全性，掌握安全口令的设置原则，以保护账户口令的安全。

2. 工作任务

(1) 使用流光扫描器探测目标主机；

(2) 使用流光扫描器制作黑客字典。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机，通过网络相连。

(2) 软件工具：流光扫描器软件。

4. 实施过程

(1) 使用流光扫描器探测目标主机

双击从网上下载的安装文件，启动其安装向导进行安装。

① 双击桌面上的 Fluxay 图标，即可进入操作界面，如图 3-1 所示。



图 3-1　流光扫描器操作界面

② 选择"文件"→"高级扫描向导"菜单项，在打开的对话框中设置 IP 起始地址和结束地址，并在"目标系统"下拉列表文本框中选择欲检测的操作系统类型。单击"获取主机名"和"PING 检查"前的按钮，使其处于选中状态，如图 3-2 所示。

③ 单击"下一步"按钮，然后选取"标准端口扫描"选项，只对常用端口进行扫描，如图 3-3 所示。

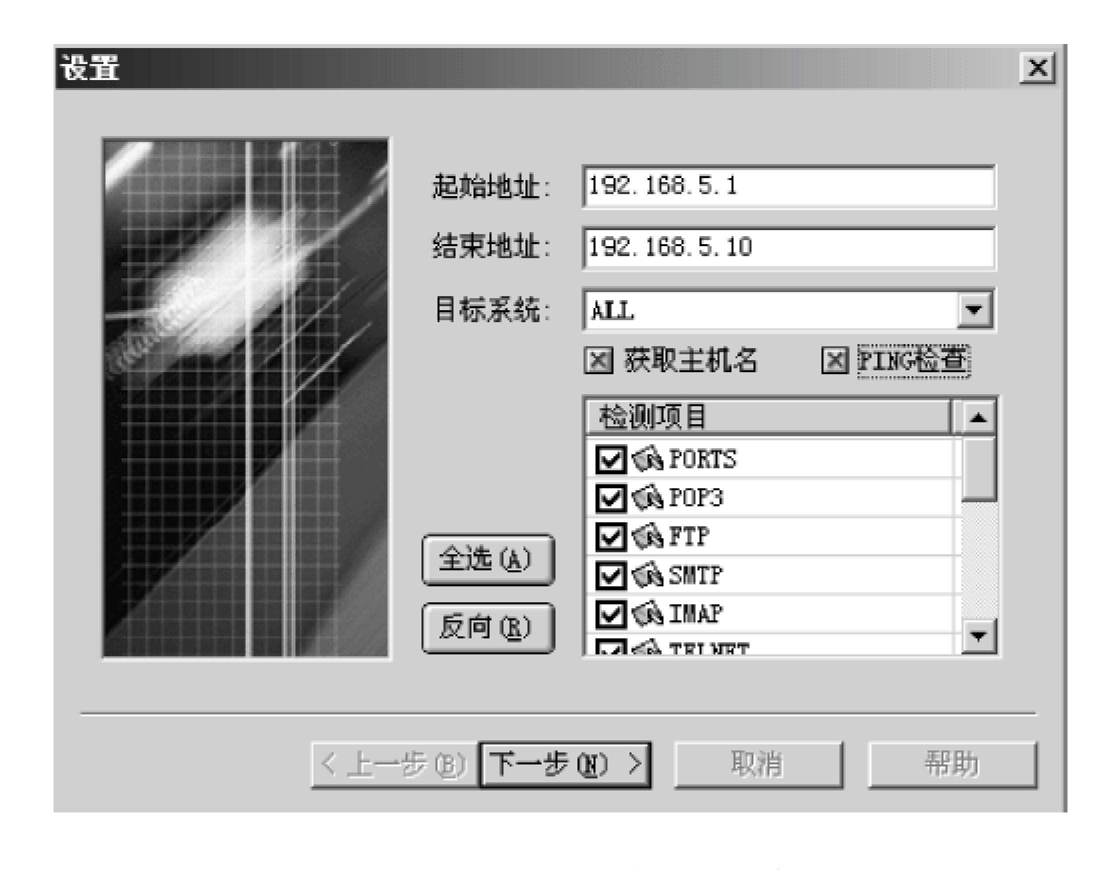


图 3-2　设置 IP 地址范围及检测项目

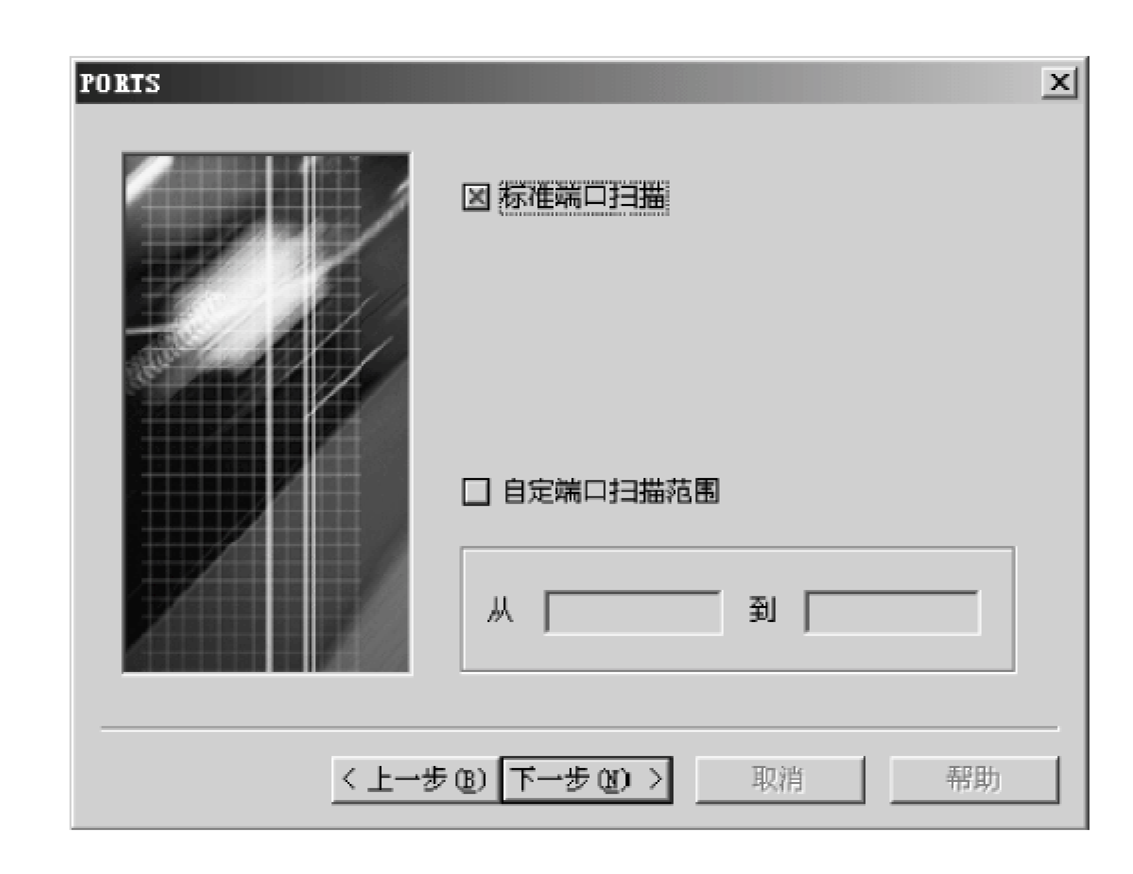


图 3-3　设置扫描端口范围

④ 单击“下一步”按钮，然后选取“获取 POP3 版本信息”及“尝试猜解用户”选项，如图 3-4 所示。

⑤ 单击“下一步”按钮，然后设置 FTP 检测的有关选项，如图 3-5 所示。

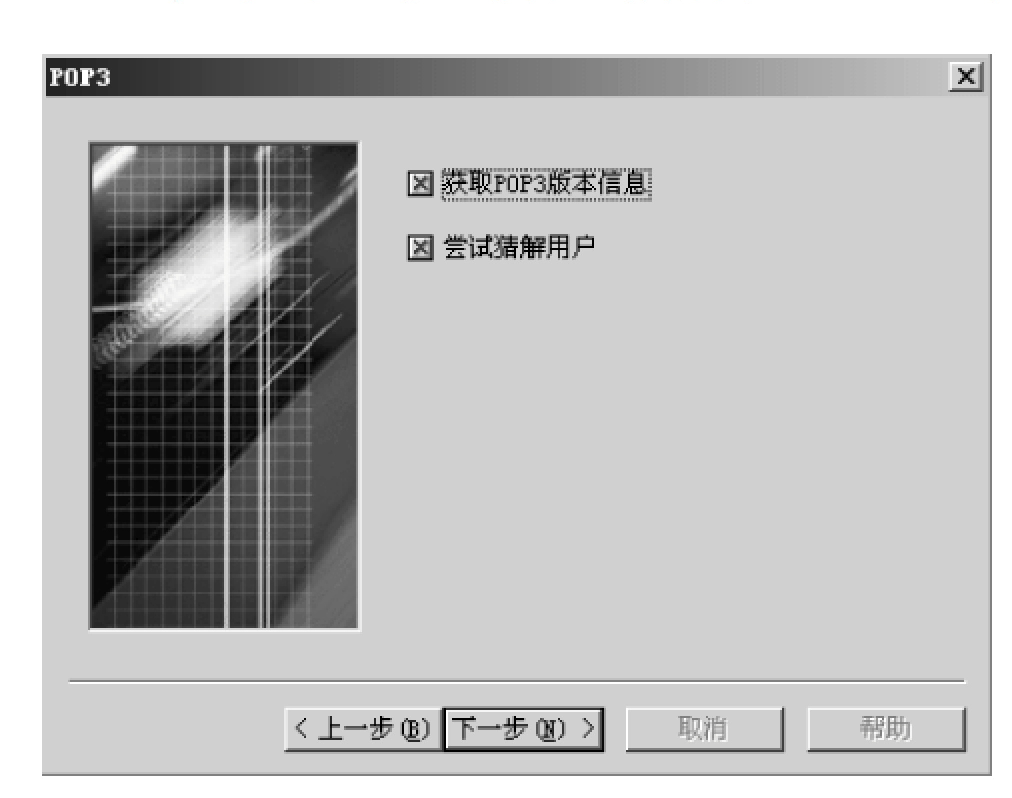


图 3-4 设置 POP3 检测选项

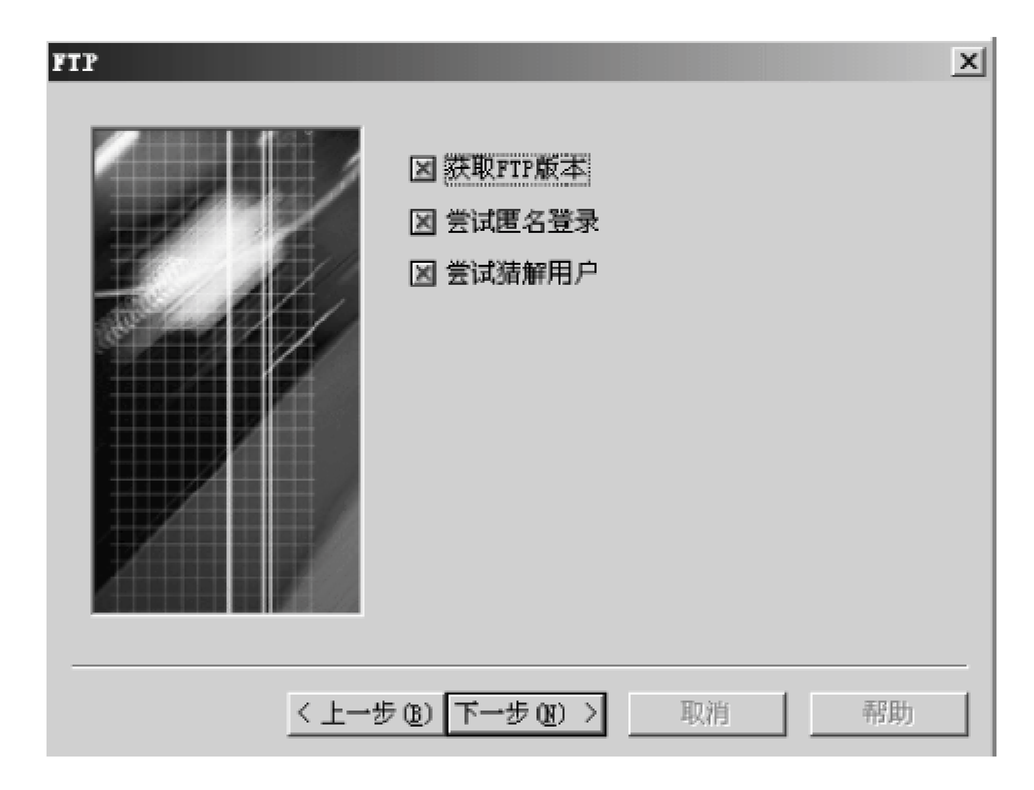


图 3-5 设置 FTP 检测选项

⑥ 单击“下一步”按钮，然后设置 SMTP 检测的有关选项，如图 3-6 所示。

⑦ 单击“下一步”按钮，然后设置 IMAP 检测的有关选项，如图 3-7 所示。

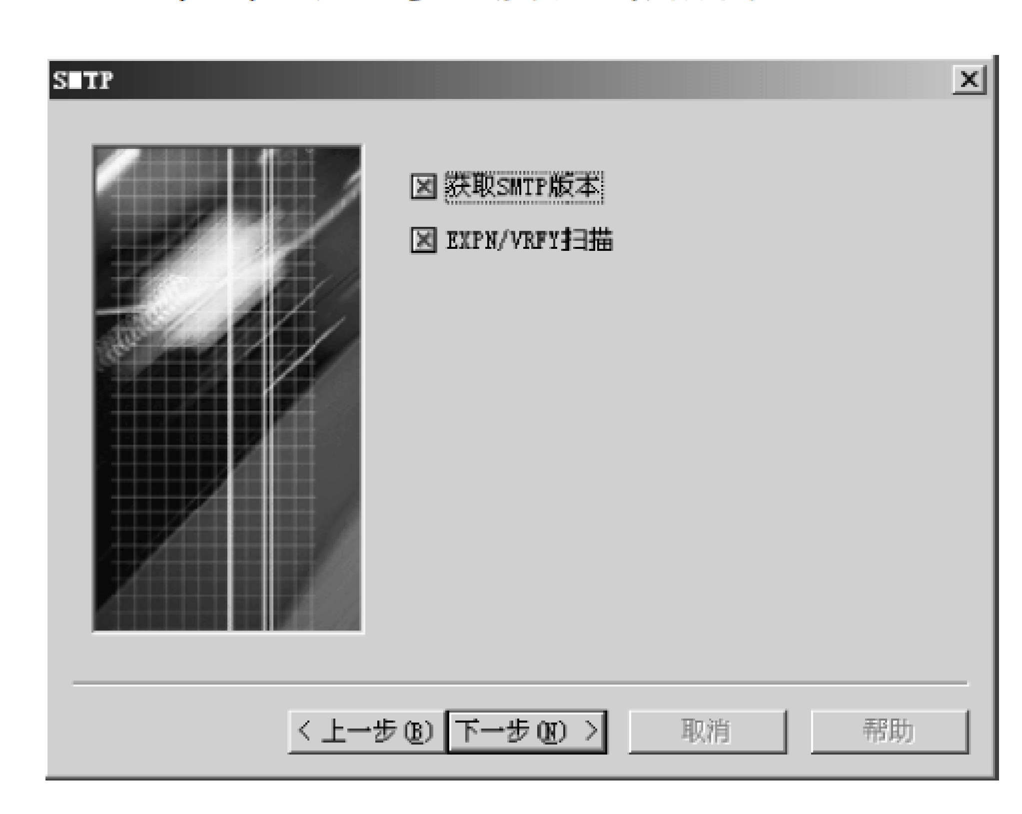


图 3-6 设置 SMTP 检测选项

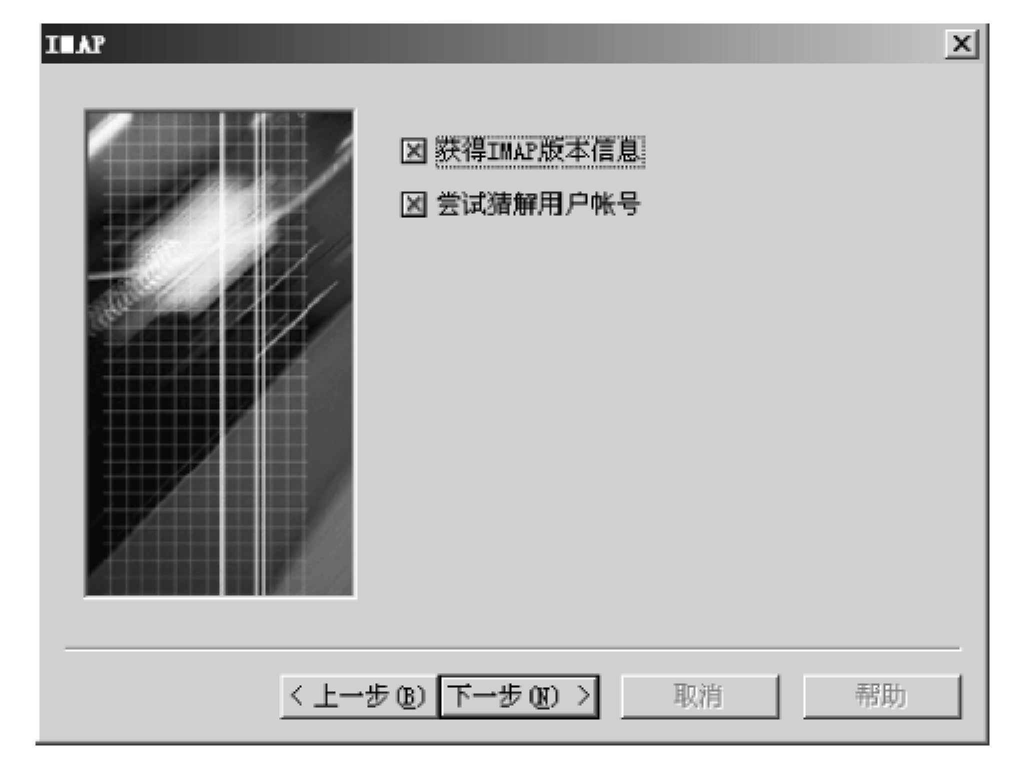


图 3-7 设置 IMAP 检测选项

⑧ 单击“下一步”按钮，然后设置 Telnet 远程溢出等选项，如图 3-8 所示。

⑨ 单击“下一步”按钮，然后在对话框中设置 CGI 的有关检测选项，如图 3-9 所示。

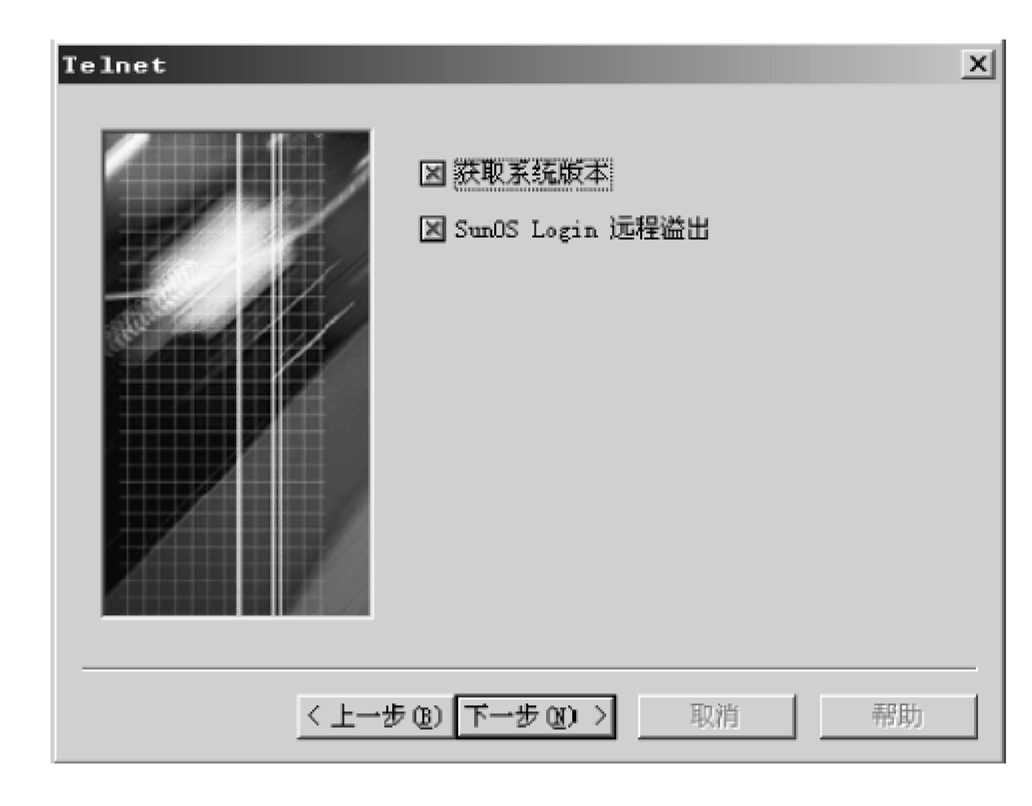


图 3-8 设置远程溢出选项

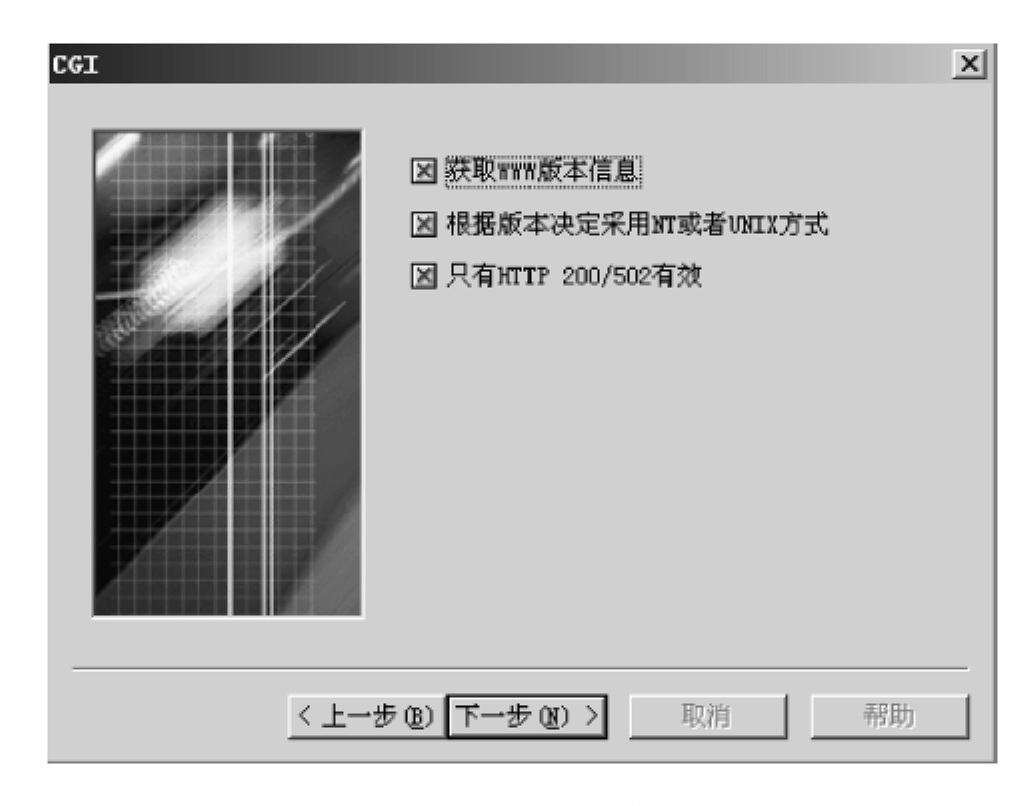


图 3-9 设置 CGI 检测选项

⑩ 单击“下一步”按钮，将显示 CGI 规则设置对话框，可选择需要扫描的 CGI 漏洞选项，如图 3-10 所示。

⑪ 单击“下一步”按钮，然后对装有 SQL 数据库的系统设置有关的漏洞扫描选项，如图 3-11 所示。



图 3-10　选择 CGI 漏洞选项

SQL
尝试通过漏洞获取密码
对SA密码进行猜解
MSSQL 2000 版本检查
上一步(B)　下一步(N)　取消　帮助

图 3-11　设置 SQL 漏洞扫描选项

⑫ 单击“下一步”按钮，然后设置有关共享资源及用户名猜解的扫描等选项，如图 3-12 所示。

⑬ 单击“下一步”按钮，然后设置 IIS 服务器的有关漏洞检测选项，如图 3-13 所示。





图 3-12　共享资源扫描等选项设置

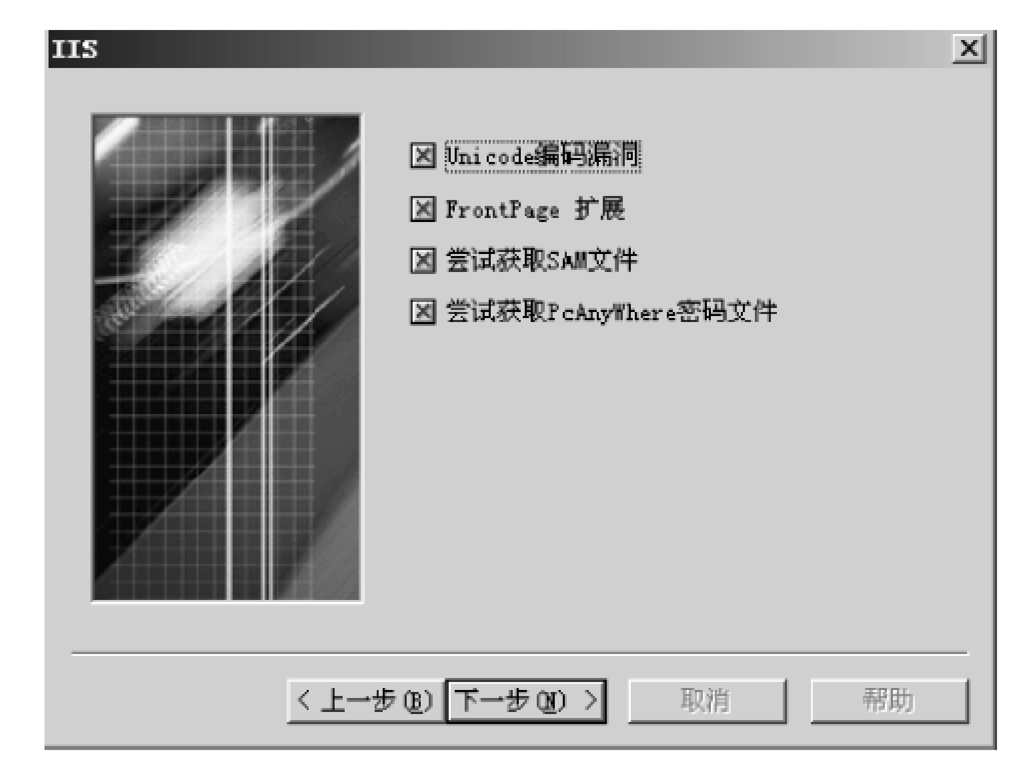


图 3-13　设置 IIS 检测选项

⑭ 单击“下一步”按钮，然后设置有关 Finger 的检测选项，如图 3-14 所示。

⑮ 单击“下一步”按钮，然后设置 RPC 的有关检测选项，如图 3-15 所示。

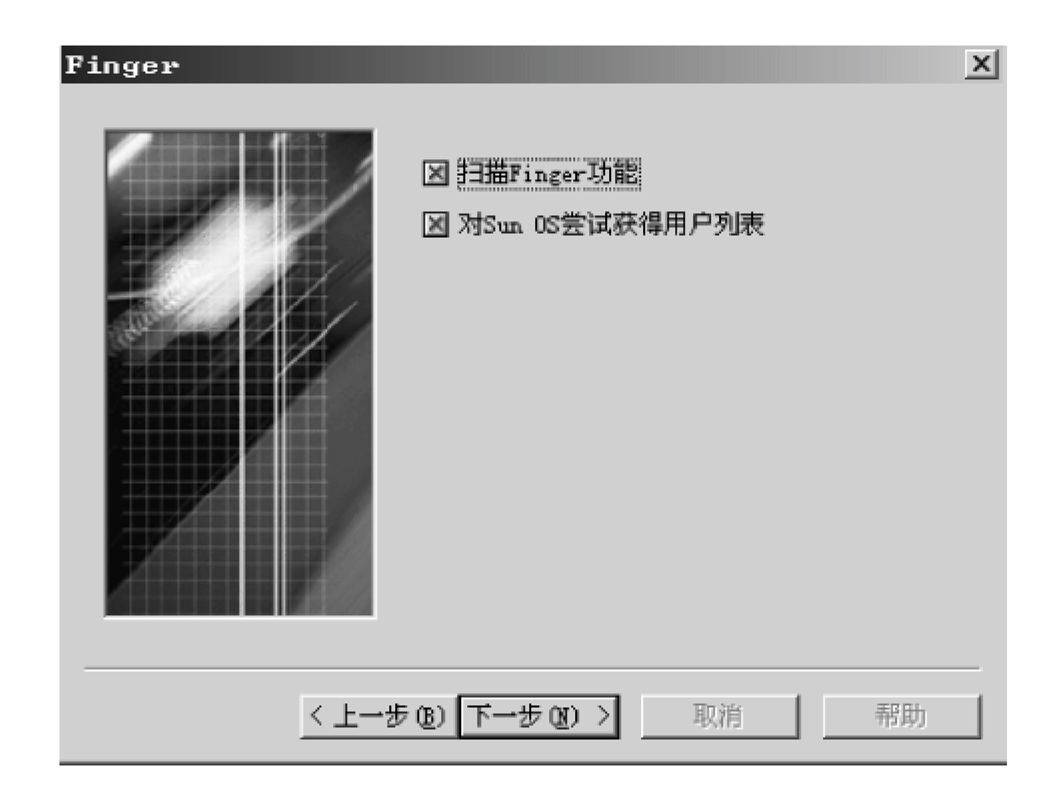


图 3-14　设置 Finger 检测选项

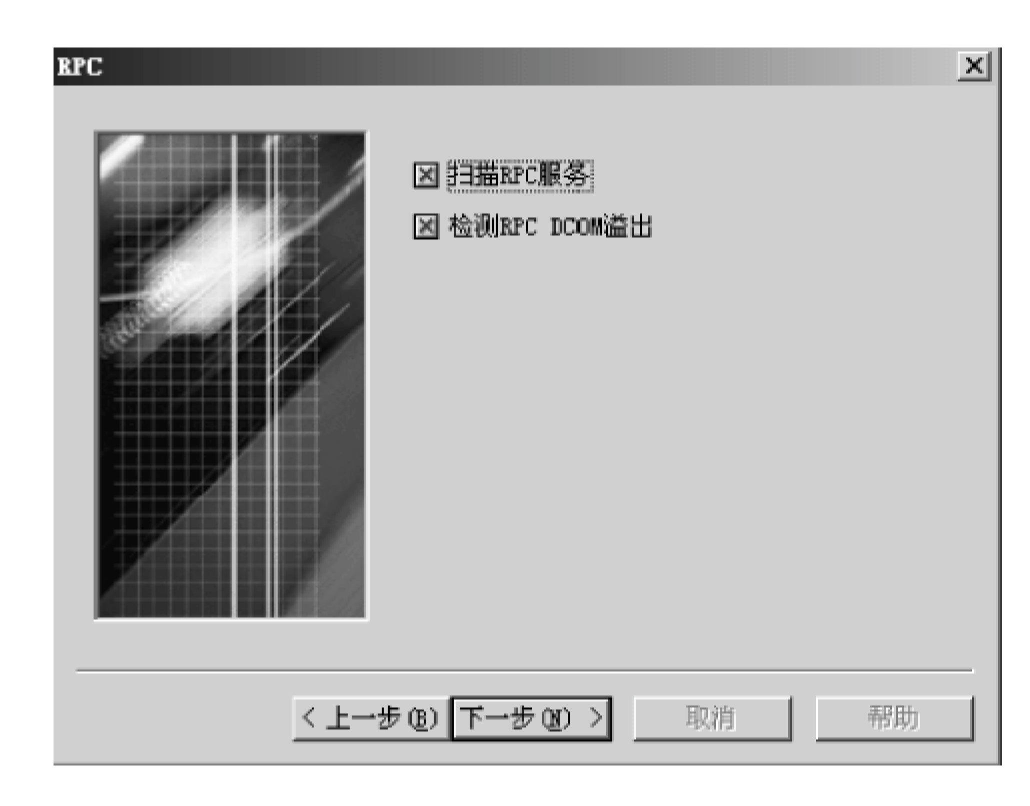


图 3-15　设置 RPC 检测选项

⑯ 单击“下一步”按钮，然后选择有关 MISC 的检测选项，如图 3-16 所示。

⑰ 单击“下一步”按钮，然后选择需要检测的系统插件漏洞类别，如图 3-17 所示。

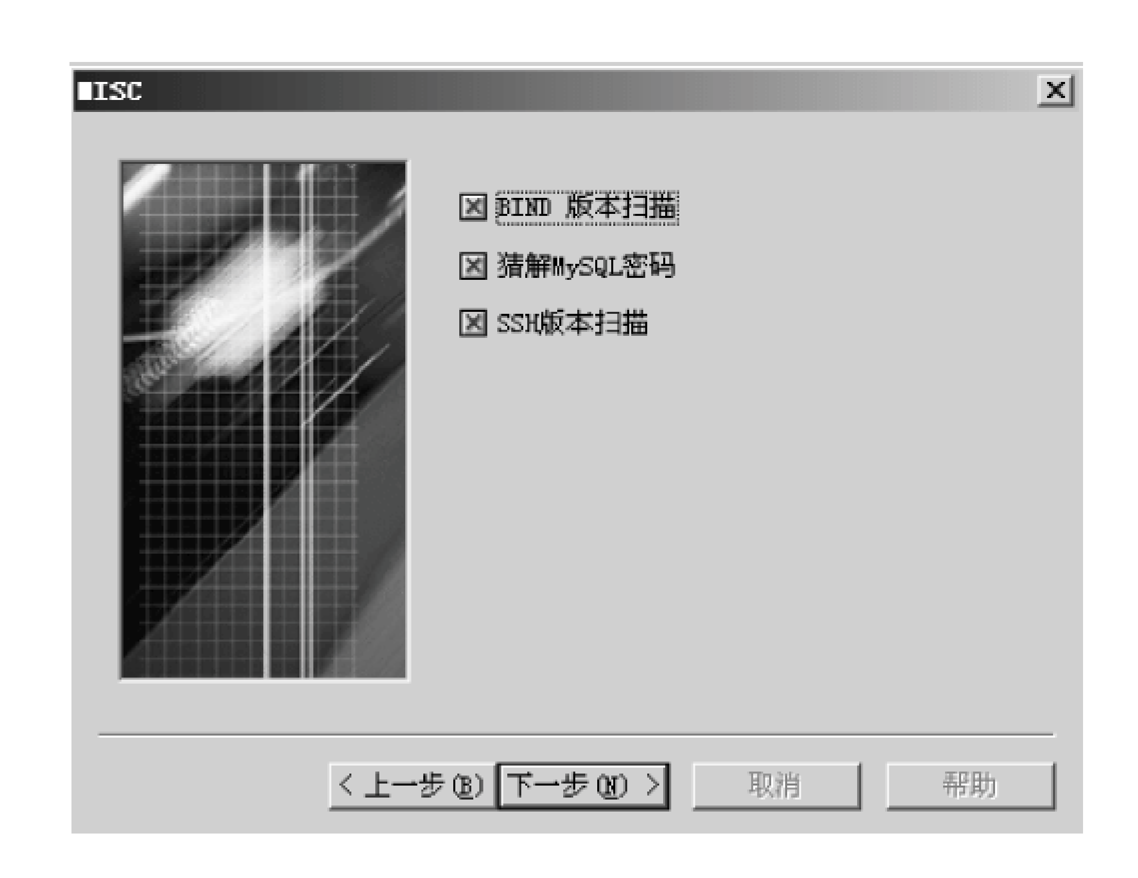


图 3-16　设置 MISC 检测选项



图 3-17　选择系统插件

⑱ 单击“下一步”按钮，然后设置使用破解用户名和密码的字典，以及扫描报告保存的路径、并发线程数量等选项，如图 3-18 所示。

⑲ 单击“完成”按钮，在显示的对话框中选择需要使用的扫描主机，如图 3-19 所示。

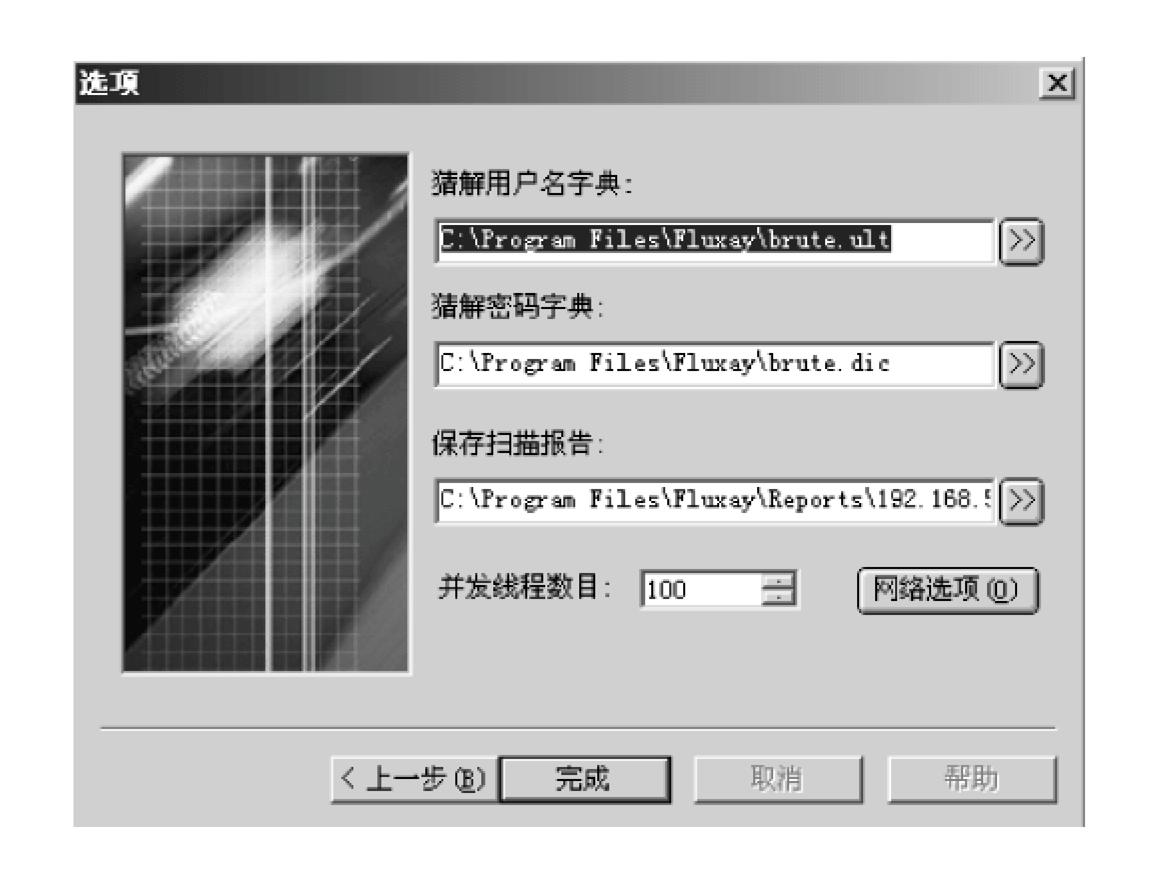


图 3-18　设置破解字典及其他选项



图 3-19　选择扫描主机

⑳ 单击“开始”按钮，流光扫描器开始扫描，如图 3-20 所示。

在扫描过程中，界面下方弹出一个“探测结果”窗口，显示扫描成功与否的信息，如图 3-21 所示。

扫描结束后，将显示如图 3-22 所示的提示框。单击“是”按钮，即可查看到扫描的最终结果，如图 3-23 所示。

(2) 使用流光扫描器制作黑客字典

使用流光扫描器制作黑客字典，可以根据用户需要任意设定包含的字母、数字、字符等内容，制作方法如下：



图 3-20　扫描中



图 3-21　探测结果

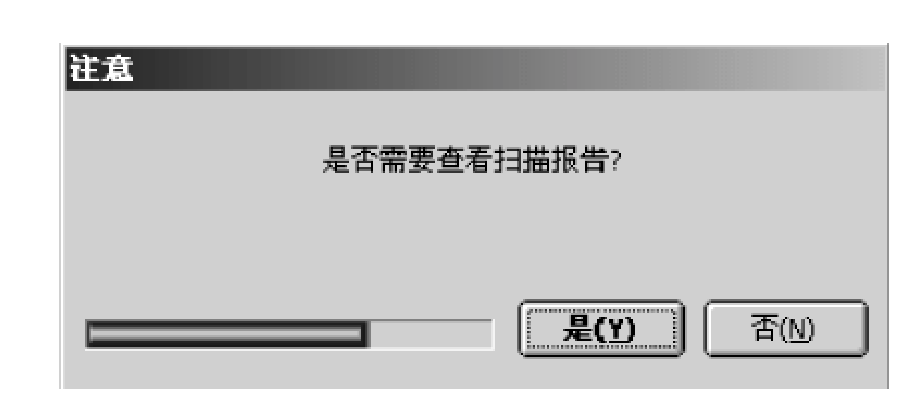


图 3-22　提示查看扫描报告



图 3-23　扫描结果

① 在流光扫描器的主界面选择“工具”→“字典工具”→“黑客字典Ⅲ-流光版”菜单项，如图 3-24 所示。



图 3-24 流光扫描器的主界面

② 在打开的对话框中选择“设置”选项卡，用户可以从中选择生成密码中包含的字母或数字及其范围，如图 3-25 所示。

③ 在“选项”选项卡中，可以设置生成的字符串是否有“字母采用大写形式”、“仅仅首字母大写”等特殊要求，如图 3-26 所示。



图 3-25 设置字典选项

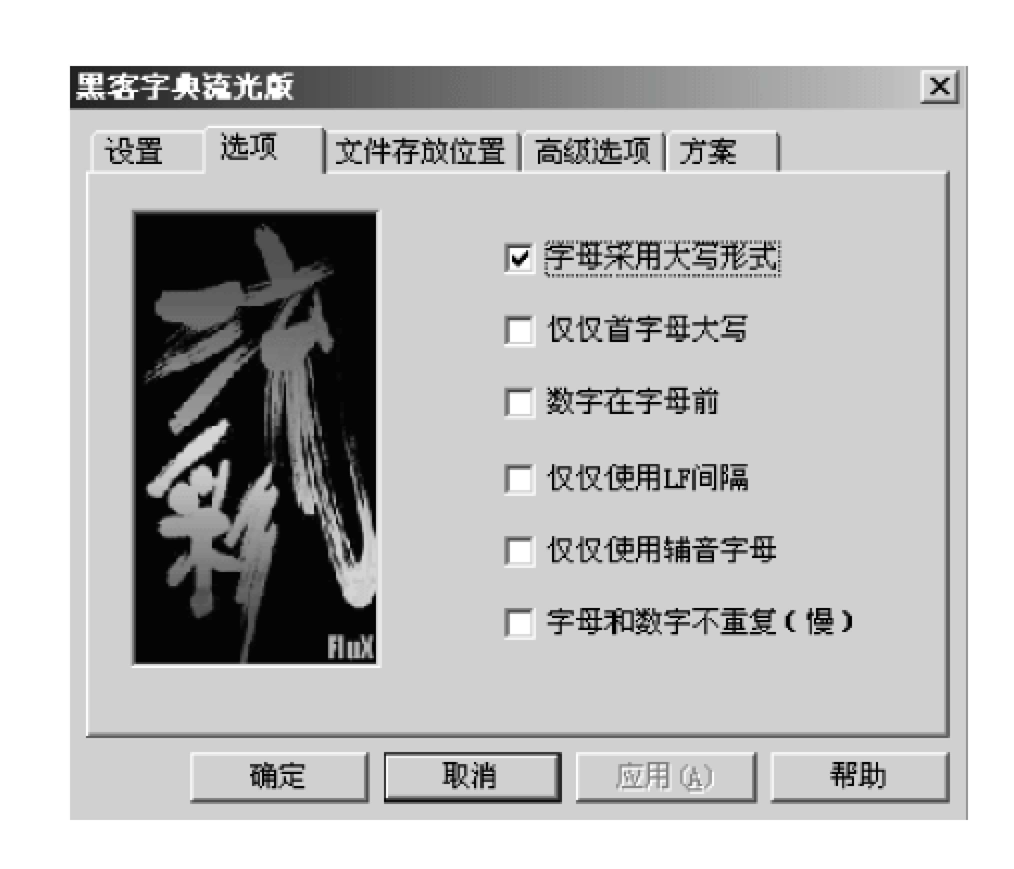


图 3-26 选项设置

④ 在“文件存放位置”选项卡中指定字典文件保存的位置，可以选择是否把大于 120KB 的字典文件进行拆分，如图 3-27 所示。

⑤ 在“高级选项”选项卡中，可以将字母、数字或字符的位置固定，如图 3-28 所示。

⑥ 单击“确定”按钮后，出现“字典属性”窗口，如图 3-29 所示，可以设置字符串的格式。如有不妥，单击“再等一会!”按钮返回设置对话框进行调整。

⑦ 单击“开始”按钮，系统开始生成字典，并显示生成字典的进度，如图 3-30 所示。



图 3-27　设置文件存放位置

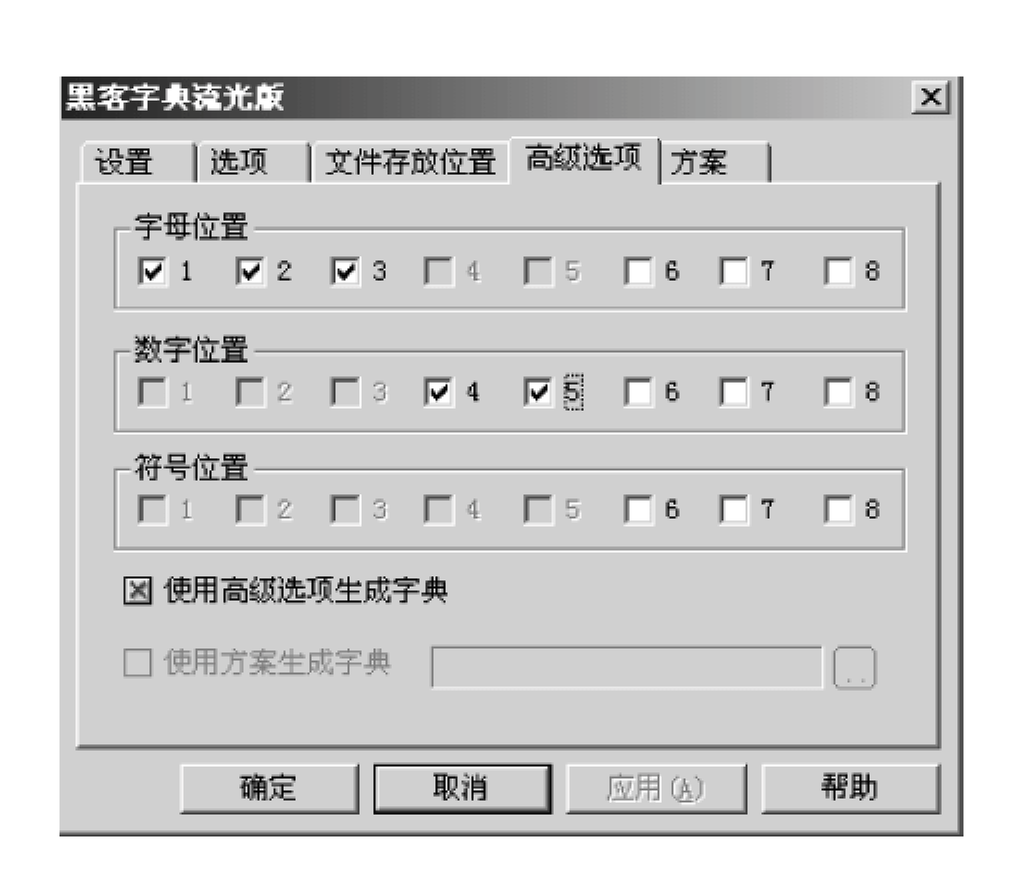


图 3-28　设置高级选项



图 3-29　高级字典属性



图 3-30　生成字典进度

3.4.2　任务 2：使用 SMBcrack 进行口令破解

1. 任务目标

通过密码破解工具的使用，了解账户的安全性，掌握安全口令的设置原则，以保护账户口令的安全。

2. 工作任务

使用 SMBcrack 工具软件进行口令破解。

3. 工作环境

（1）两台预装 Windows Server 2003/XP 的主机，通过网络相连。

（2）软件工具：SMBcrack。

4. 实施过程

SMBcrack 工具软件需要在 DOS 命令行窗口运行，SMBcrack 的命令格式为

SMBcrack <IP> <Username> <Password file> <Port>

其中，IP 是目标主机的 IP 地址；Username 是目标主机需要破解的账号；Password file 是字典文件，如图 3-31 所示。

```
命令提示符
SMB Cracker V3-Protype for Fluxay 5, by netXeyes 2002

SMBCrack <IP> <Username> <Password file> [Port]

C:\SMBCrack>
```

图 3-31 SMBcrack 工具软件

假定 SMBcrack 工具软件在 C 盘 hk 目录，要先把字典文件复制到 hk 目录中，再按下列步骤操作。

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。在命令提示符窗口，输入“cd\”后按“Enter”键回到 C 盘根目录，然后输入“cd SMBcrack”；按“Enter”键后输入“smbcrak 192.168.5.2 administrator 1.dic”，再按“Enter”键，如图 3-32 所示。

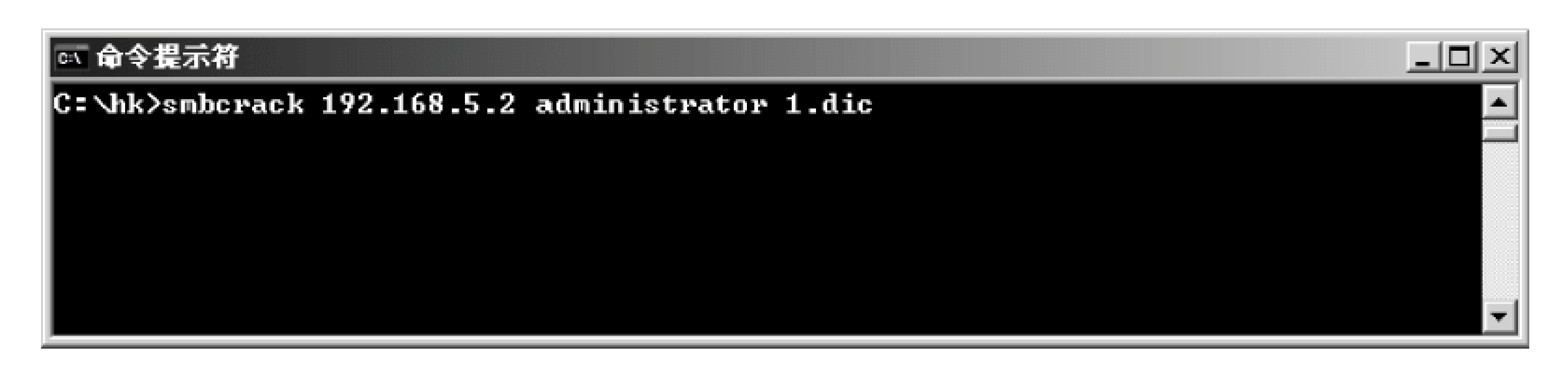


图 3-32 SMBcrack 命令

② 开始口令破解，命令提示符窗口显示破解的进度，如图 3-33 所示。

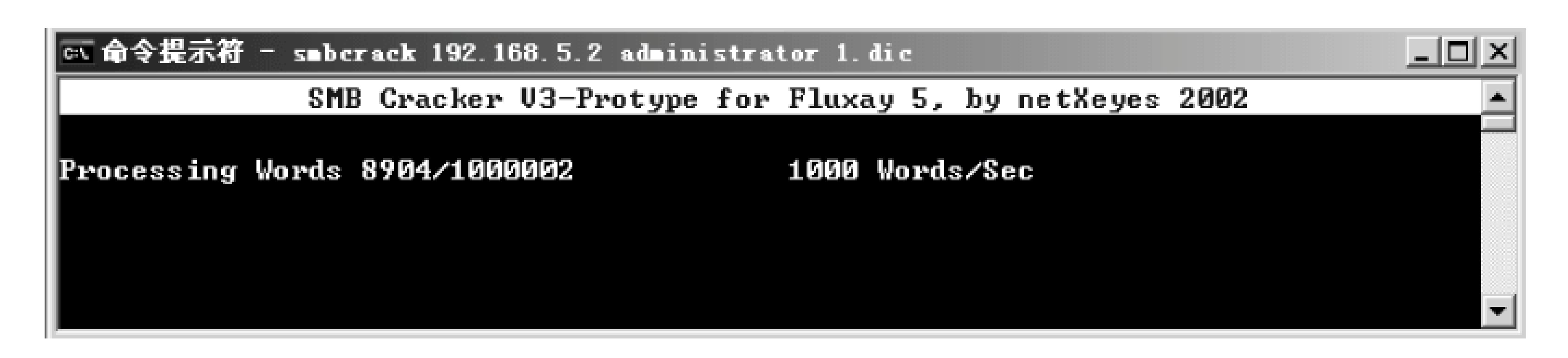


图 3-33 口令破解中

③ 目标主机 192.168.5.2 的用户名是“administrator”，密码是“123321”，口令破解的实验结果如图 3-34 所示。

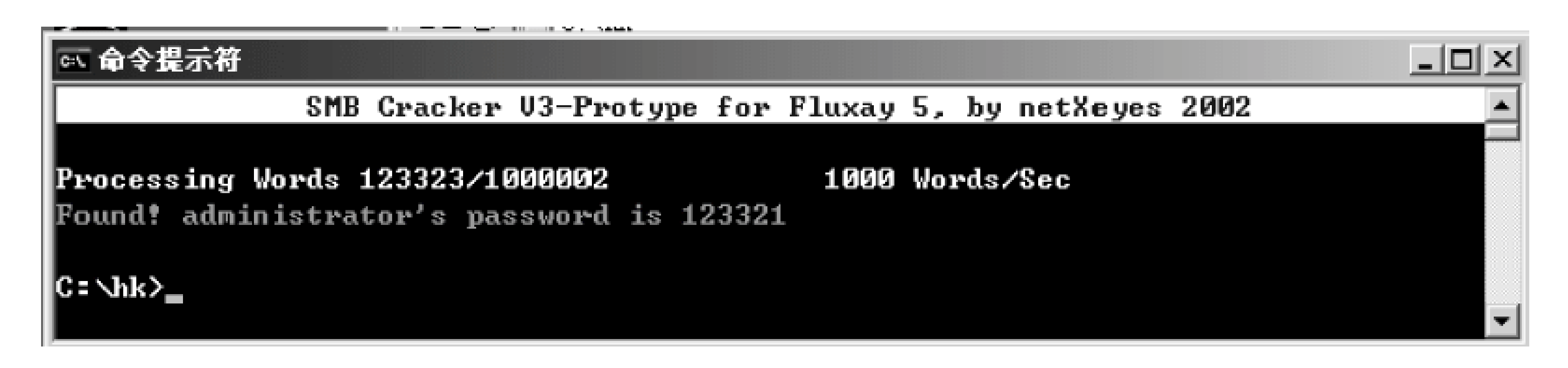


图 3-34 实验结果

3.5 常见问题解答

1. 如何防止账户密码被破解？

答：设定密码时最好不要使用名字的拼音或生日数字的组合，最好使用无意义的数字

和字母组合，并且位数尽量多，经常更换，防止黑客破解；对不同网站和程序要使用不同的密码，防止黑客破译；网上购物时，不论出于何种原因，都不允许自己的信用卡资料被商家存储；只向有安全保证的网站发送信用卡号码，并留意浏览器底部显示的挂锁图标或钥匙形图标。

2. 什么叫弱口令扫描？

答：弱口令是指仅包含简单数字和字母的口令，例如123、abc。这样的口令很容易被破解，从而使用户的计算机面临风险，因此不推荐使用。用户的口令最好由字母、数字和符号混合组成，并且至少要达到8位长度。弱口令可能存在于自己的计算机系统中，也可能存在于用户在网络上的注册信息中，如计算机的登录口令、QQ密码等。对于在网络上注册的重要信息，如网上银行登录口令、邮箱的登录口令等，设置得过于简单，就可能被人破解，从而造成重大损失，所以用户需要特别注意。

3.6 过关练习

一、选择题

1. 网络攻击的发展趋势是(　　)。

A. 黑客技术与网络病毒日益融合　　B. 攻击技术日益先进
C. 病毒攻击　　D. 黑客攻击

2. 通过非直接技术攻击称为(　　)攻击手法。

A. 会话劫持　　B. 社会工程学　　C. 特权提升　　D. 应用层攻击

3. 关于“攻击工具日益先进，攻击者需要的技能日趋下降”的观点不正确的是(　　)。

A. 网络受到攻击的可能性越来越大　　B. 网络受到攻击的可能性越来越小
C. 网络攻击无处不在　　D. 网络风险日益严重

4. 一次字典攻击能否成功，很大因素取决于(　　)。

A. 字典文件　　B. 计算机速度　　C. 网络速度　　D. 黑客学历

5. 打电话请求密码属于(　　)攻击方式。

A. 木马　　B. 社会工程学　　C. 电话系统漏洞　　D. 拒绝服务

二、简答题

1. 常用的口令破解工具有哪些？
2. 什么叫弱口令？

三、操作题

1. 利用流光软件制作黑客字典，要求密码由3位字母(a～z)和2位数字(0～9)组成，首字母为大写，数字在字母之后。

2. 利用流光软件制作黑客字典，要求密码由3位字母(a～z)和2位数字(0～9)组成，首字母为大写，数字在第3、4位，字母在第1、2、5位。

3. 利用流光软件制作黑客字典，要求密码由6位字母(a～z)和2位数字(0～9)组成，首字母为大写，数字在第2、4位，字母在第1、3、5、6、7、8位。

工作任务四

网络监听工具的使用

4.1 用户需求与分析

网络监听工具是一把双刃剑。在网络管理员手中,网络监听工具能帮助用户监控网络流量,更好地管理网络;在黑客手中,网络监听工具能够捕获计算机用户因为疏忽带来的漏洞,成为一个危险的网络间谍。掌握网络监听工具的使用方法对于学习黑客入侵知识会起到事半功倍的效果。

4.2 预 备 知 识

4.2.1 网络监听的原理

网络嗅探器或网络监听技术在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用,因此一直备受网络管理员的青睐并逐渐发展完善。所谓监听技术,就是在互相通信的两台计算机之间通过技术手段插入一台可以接收并记录通信内容的设备,并最终实现对通信双方的数据记录。一般要求用作监听途径的设备不能造成通信双方的行动异常或者链接中断等,即监听方不能参与通信中任何一方的通信行为,仅仅是被动地接收、记录通信数据,而不能对其进行篡改。

监听的弱点是它要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系,或者数据包能经过路由选择到达对方,即一个逻辑上的三方连接。能实现这个条件的只有两种情况:监听方与通信方位于同一物理网络,如局域网,或者是监听方与通信方存在路由或接口关系,例如通信双方的同一网关、连接通信双方的路由设备等。因此嗅探技术不太可能在公共网络设备上使用,所以当今最普遍的嗅探行为并不是发生在互联网上,而是发生在各个或大或小的局域网中,因为它满足监听技术的必要条件:监听方与通信方位于同一物理网络。

4.2.2 常见网络监听工具介绍

网络监听工具又称为网络嗅探器,是一种监视和收集网络中各种数据信息的软件,利用它,通过网卡可以随意对网络中的信息进行查看、监视以及截获,它是黑客最得力的信息收集工具。

网络监听工具分为软件和硬件两种,软件的有 Sniffer Pro、Wireshark、Network Monitor等,优点是易于安装部署,易于学习、使用和交流;缺点是无法抓取网络上所有的传输,在某些情况下无法真正了解网络的故障和运行情况。硬件的网络监听工具通常称为协议分析仪,一

般是商业性的，价格比较昂贵，但会支持各种扩展的链路捕获能力以及高性能的数据实时捕获分析功能。

下面介绍几种最常见的网络监听工具软件。

1. Sniffer 嗅探器

Sniffer 嗅探器即 Sniffer Pro，是目前黑客最常用的网络嗅探软件。它是一款由 NAT 公司推出的网络协议分析软件，功能包括捕获网络流量，基于各种网络协议分析网络数据，实时监控单个工作站、会话或者网络中任何一部分详细的网络利用情况和错误统计，利用专家分析系统诊断问题，可以解码至少 450 种协议，支持主要的 LAN、WAN 和网络技术，提供在位和字节水平过滤数据包的能力。它可以在各种 Windows 平台上运行，解决网络中存在的问题。

2. Wireshark 工具

Wireshark（前称 Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是捕捉网络数据包，并尽可能显示出最为详细的数据包内容。在过去，网络数据包分析软件或者非常昂贵，或者专门属于营利用的软件。Wireshark 的出现改变了这一切。在 GNUGPL 通用许可证的保障下，使用者可以免费取得软件及其源代码，并拥有对源代码修改的权利。Wireshark 是目前全世界最广泛的网络封包分析软件之一。

4.3 方案设计

方案设计如表 4-1 所示。

表 4-1　方案设计

任务名称	网络监听工具的使用
任务分解	1. Sniffer 嗅探器的使用 (1) Sniffer Pro 的安装 (2) Sniffer Pro 的配置 (3) 用 Sniffer Pro 捕获数据包 2. Wireshark 工具的使用 (1) 设置 Wireshark 的过滤规则 (2) 指定过滤器 (3) 用 Wireshark 捕获数据包
能力目标	1. 能顺利安装 Sniffer Pro 软件 2. 能对 Sniffer Pro 进行配置 3. 能使用 Sniffer Pro 软件捕获数据包 4. 能使用 Sniffer Pro 软件捕获远程登录的用户名和密码 5. 能使用 Sniffer Pro 软件捕获 FTP 登录的用户名和密码 6. 能设置 Wireshark 的过滤规则 7. 能为 Wireshark 指定过滤器 8. 能使用 Wireshark 捕获数据包 9. 能用 Wireshark 嗅探 FTP 登录，并从捕获数据中分析出登录的账号和密码 10. 能使用科来网络分析系统统计网络流量 11. 能使用科来网络分析系统了解网络流量应用组成以及如何被利用

续表

知识目标	1. 了解网络监听的原理 2. 熟悉常用的网络监听工具的优点及缺点 3. 了解 Sniffer 嗅探器的作用 4. 了解 Wireshark 工具软件的作用
素质目标	1. 具有良好的团队协作和沟通交流能力 2. 培养良好的职业道德 3. 掌握网络安全行业的基本情况 4. 树立较强的安全、节约、环保意识 5. 培养创新能力

4.4 任 务 实 施

4.4.1 任务 1：Sniffer 嗅探器的使用

1. 任务目标

掌握 Sniffer Pro 的安装方法，熟练掌握 Sniffer Pro 的几个主要功能，查看网络流量、主机、协议和网络连接的方法；能选择监听的网卡，查看捕获的报文，并能对捕获的数据包进行专家分析、解码分析和统计分析；能对基本捕获条件、高级捕获条件和任意捕获条件进行设置。

2. 工作任务

(1) Sniffer Pro 的安装；

(2) Sniffer Pro 的配置；

(3) 用 Sniffer Pro 捕获数据包。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机，通过网络相连。

(2) 软件工具：Sniffer Pro 软件。

4. 实施过程

(1) Sniffer Pro 的安装

① 双击安装程序，进入 Sniffer Portable 4.7.5 的安装界面，如图 4-1 所示。

② 不断单击“下一步”按钮，出现许可协议，单击“同意”按钮。

③ 在用户信息对话框中输入姓名和公司。

④ 单击“下一步”按钮，然后选择并设置安装的路径，再单击“下一步”按钮进行安装。默认安装在 C:\Program Files\NAI\SnifferNT 目录中，可以通过单击旁边的“Browse”按钮修改路径。为了更好地使用，还是使用默认路径来安装。

⑤ 在“Sniffer Pro User Registration”对话框中填写个人信息，包括名字、行业、电子邮箱等，如图 4-2 所示。填写时注意格式，E-mail 地址要符合规范，需要带有“@”。

⑥ 填写个人联系方式，包括地址、城市、国家、邮编、电话号码等。填写完毕后单击“下



图 4-1　安装界面

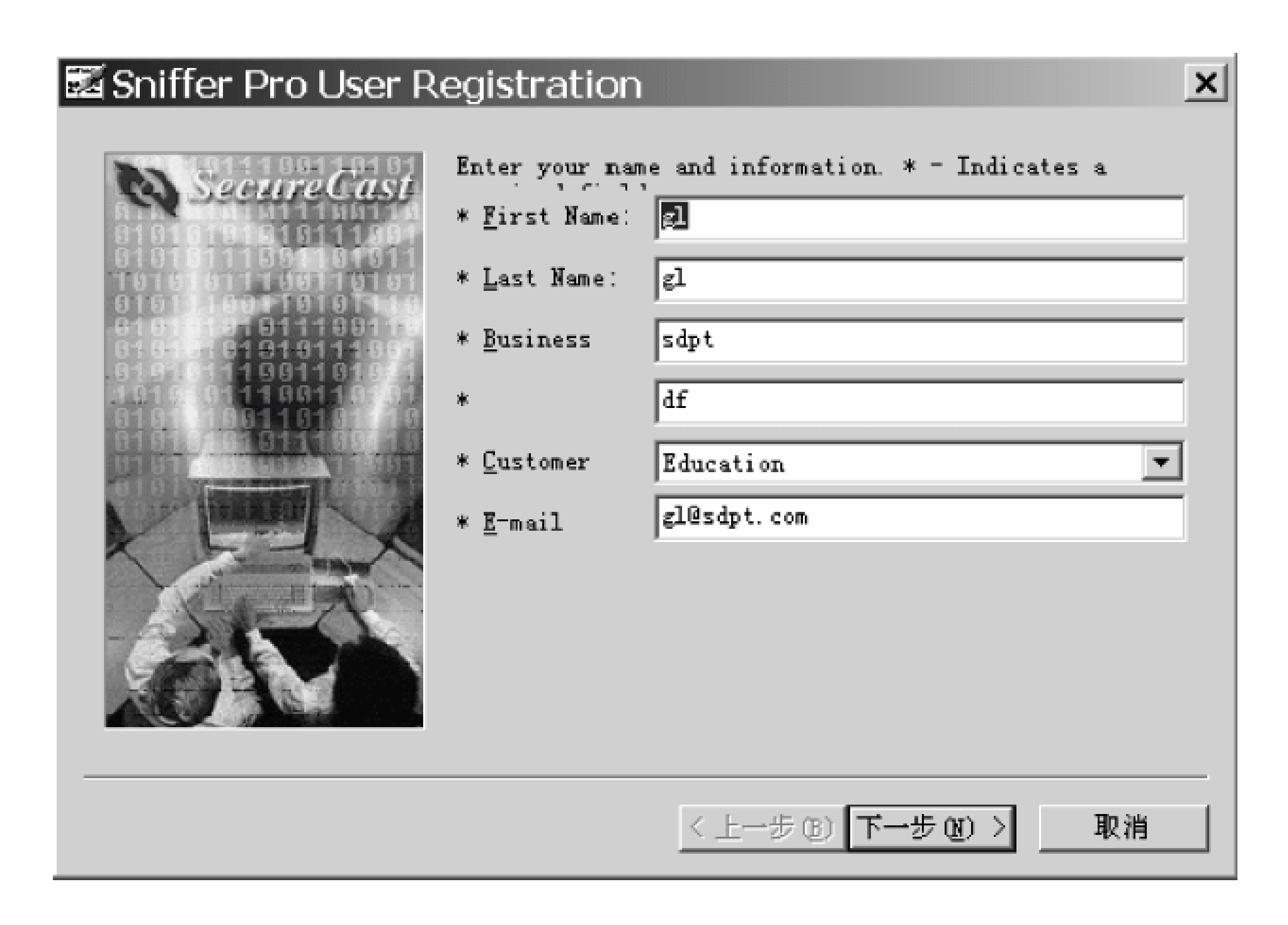


图 4-2　注册 Sniffer Pro

一步”按钮，注意字母和数字要区分。

⑦ 接下来询问安装者是如何了解本软件的。最后的“Sniffer Serial Number”栏用于填写序列号。

⑧ 设置网络连接状况。只要不是通过“代理服务器”上网的用户都可以选择第一项“Direct Connection to the Internet”，然后单击“下一步”按钮，如图 4-3 所示。

⑨ 接着是通过网络注册的提示。暂时不注册并不妨碍使用软件。

⑩ 单击“下一步”按钮，出现注册结果，单击“完成”按钮。

⑪ 软件提示重启计算机。因为 Sniffer Pro 需要将网卡的监听模式切换为“混杂”，不重启计算机无法实现切换功能。

⑫ 重启计算机后便完成了安装。根据需要，决定是否安装汉化补丁。

(2) Sniffer Pro 的配置

Sniffer Pro 是非常优秀的协议分析软件，又是非常优秀的嗅探器，它利用以太网特性把

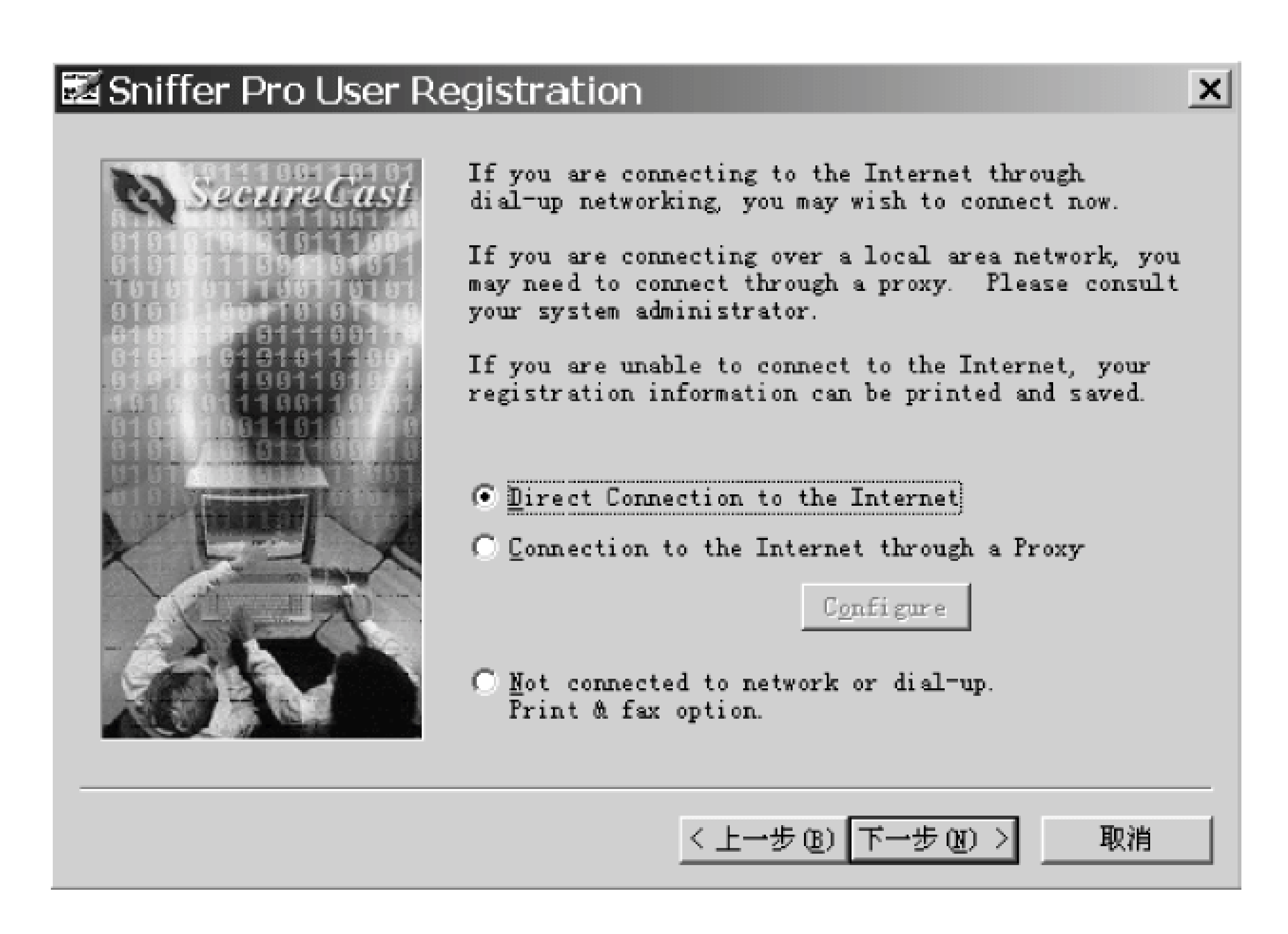


图 4-3　设置网络连接

网络适配卡(NIC,一般为以太网卡)置为混杂模式状态后,能接收传输在网络上的每一个信息包。Sniffer Pro 的配置步骤如下:

① 安装完成后,单击"Dashboard(仪表板)"图标,主界面出现 3 块表。第一块表显示网络的使用率(Utilization);第二块表显示网络每秒钟通过的包数量(Packets);第三块表显示网络的每秒错误率(Errors)。红色部分显示的是根据网络要求设置的上限,如图 4-4 所示。



图 4-4　Sniffer Pro 程序主界面

② 单击"Host table(主机列表)"图标,出现所有在线的本网主机地址以及联到外网的外网服务器地址,如图 4-5 所示。

③ 若想了解某台计算机的上网情况,只需双击该计算机的 IP 地址,即弹出该计算机网络连接情况的界面,如图 4-6 所示。

④ 单击"Detail(协议分布)"图标,将显示整个网络的协议分布情况,可清楚地看出哪台计算机运行了哪些协议,如图 4-7 所示。如果在图 4-6 所示界面上单击,则显示指定计算机的情况。

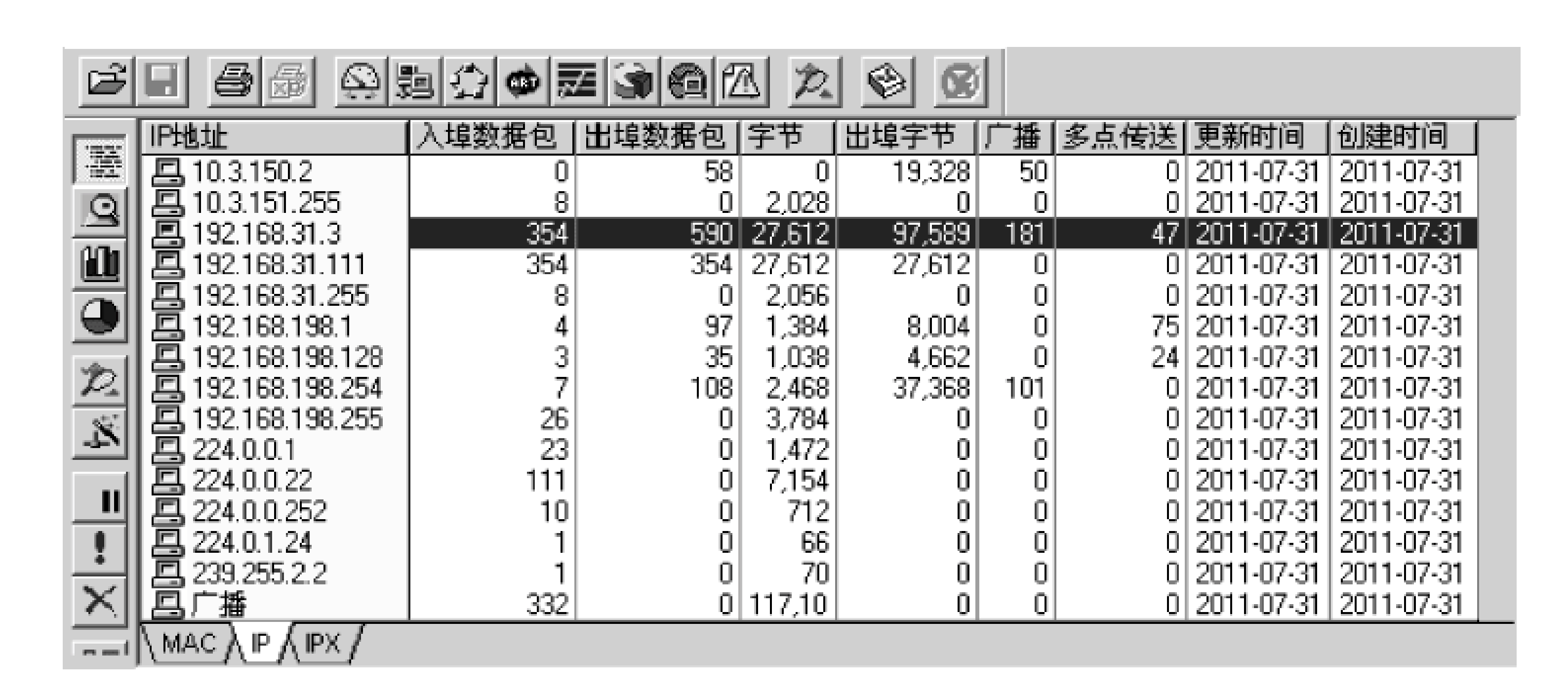


图 4-5　主机列表(1)

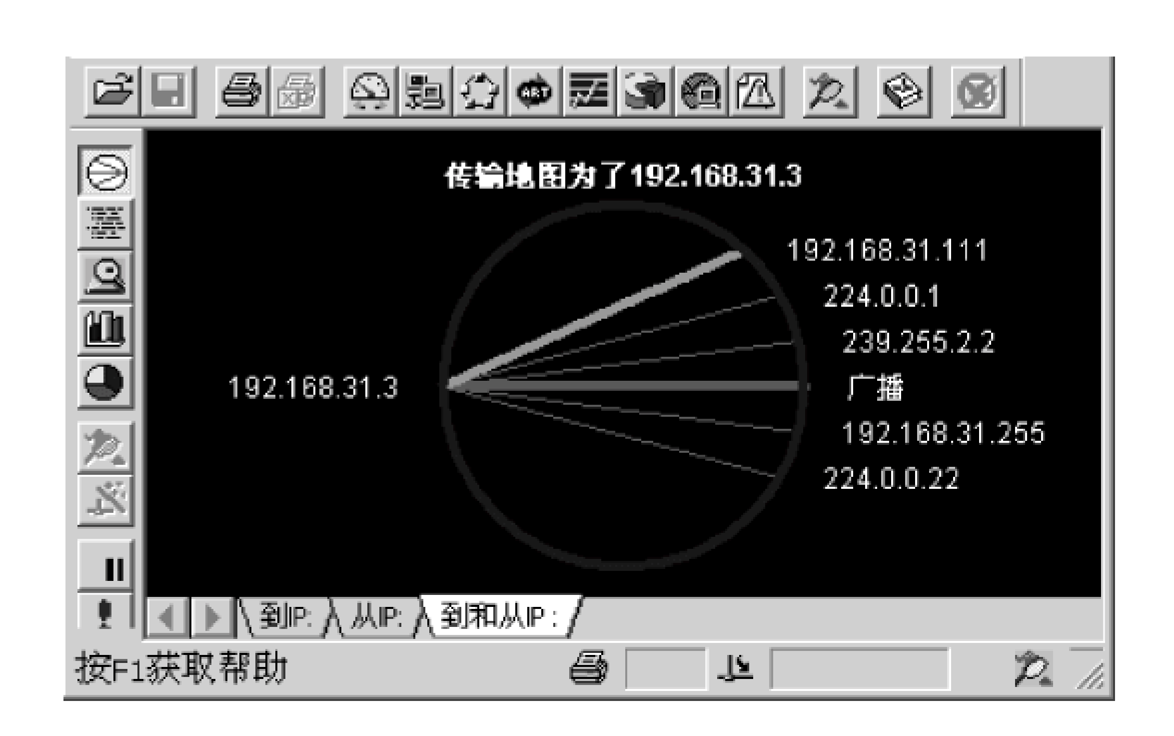


图 4-6　某台计算机的连接情况示意图

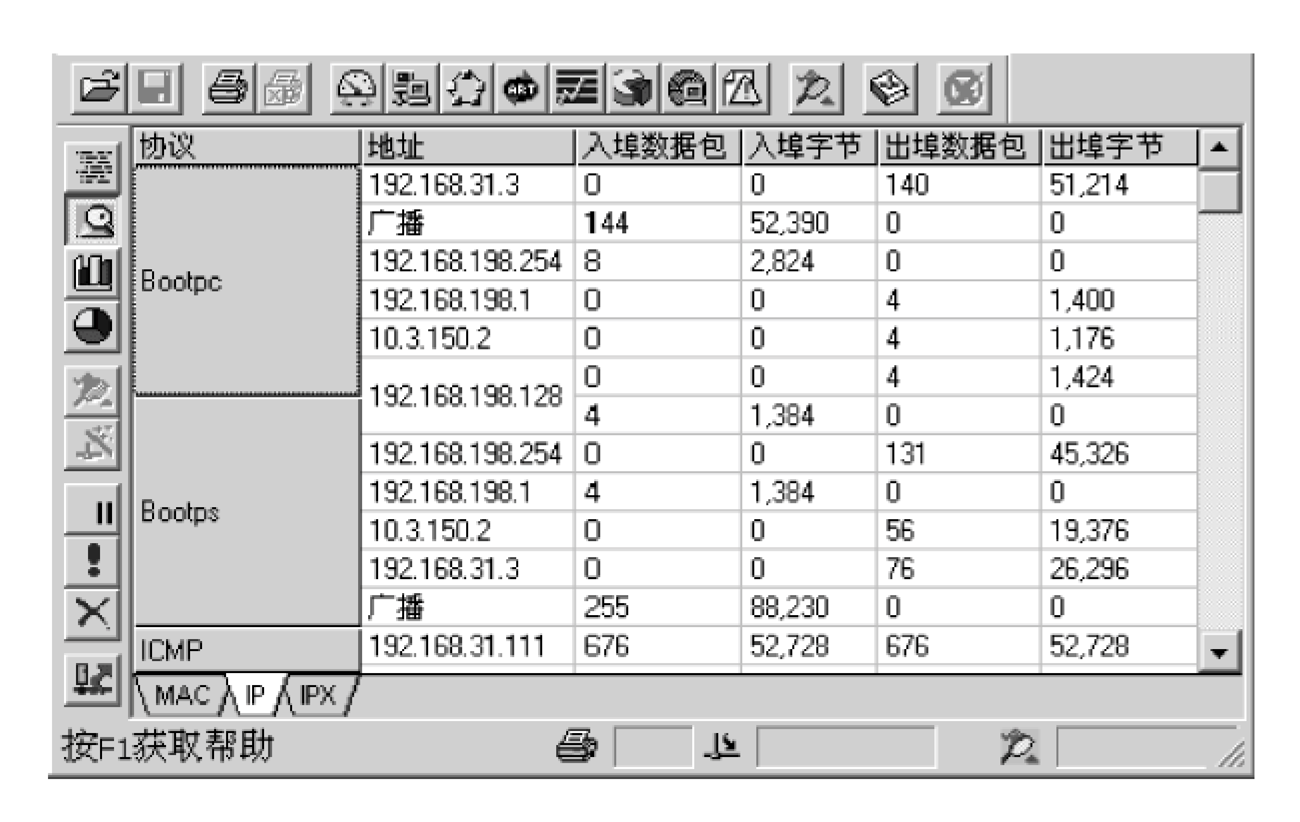


图 4-7　网络中的协议分布

⑤ 单击“Bar(流量列表)”图标,将显示整个网络中计算机所用带宽前 10 名的情况。显示方式可以是柱状图或饼状图,如图 4-8 所示。

⑥ 单击“Matrix(网络连接)”图标,会出现全网的连接示意图。图中,绿线表示正在发生的网络连接,蓝线表示过去发生的连接。将鼠标放在线上可以看出连接情况。将鼠标右键在弹出的菜单中单击,可选择放大此图,如图 4-9 所示。

(3) 用 Sniffer Pro 捕获数据包

① 首次打开 Sniffer Pro 的时候,会弹出选择网卡对话框,其中会自动显示本机当前拥

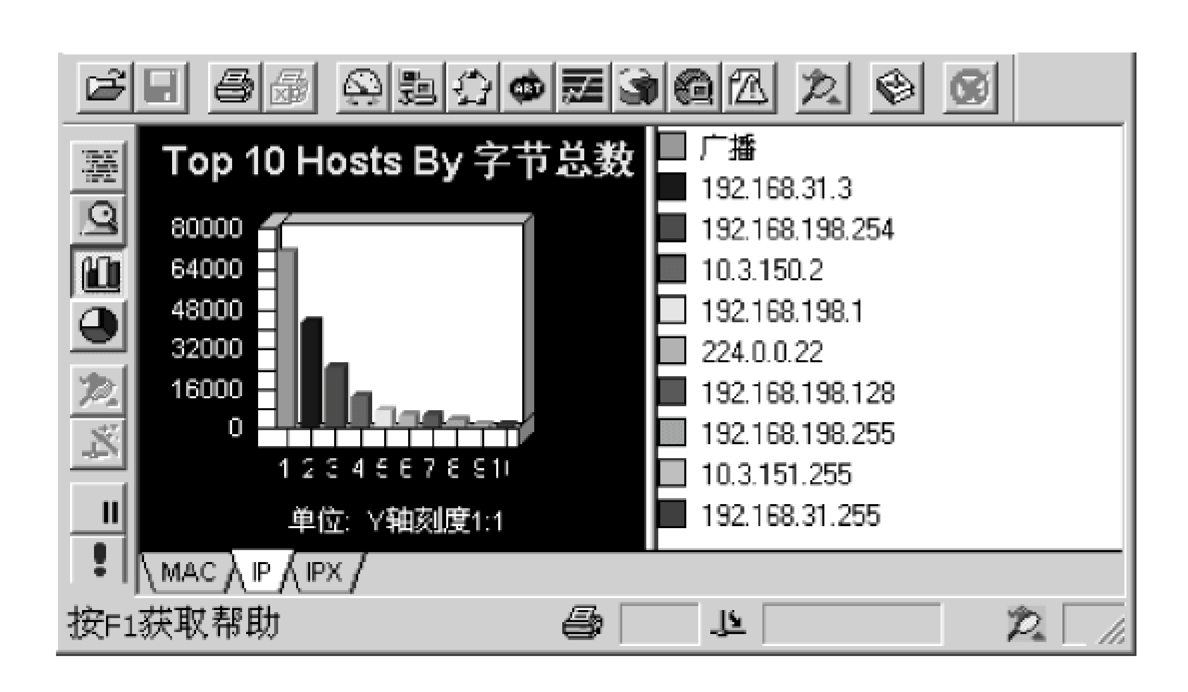


图 4-8　网络中带宽显示柱状图

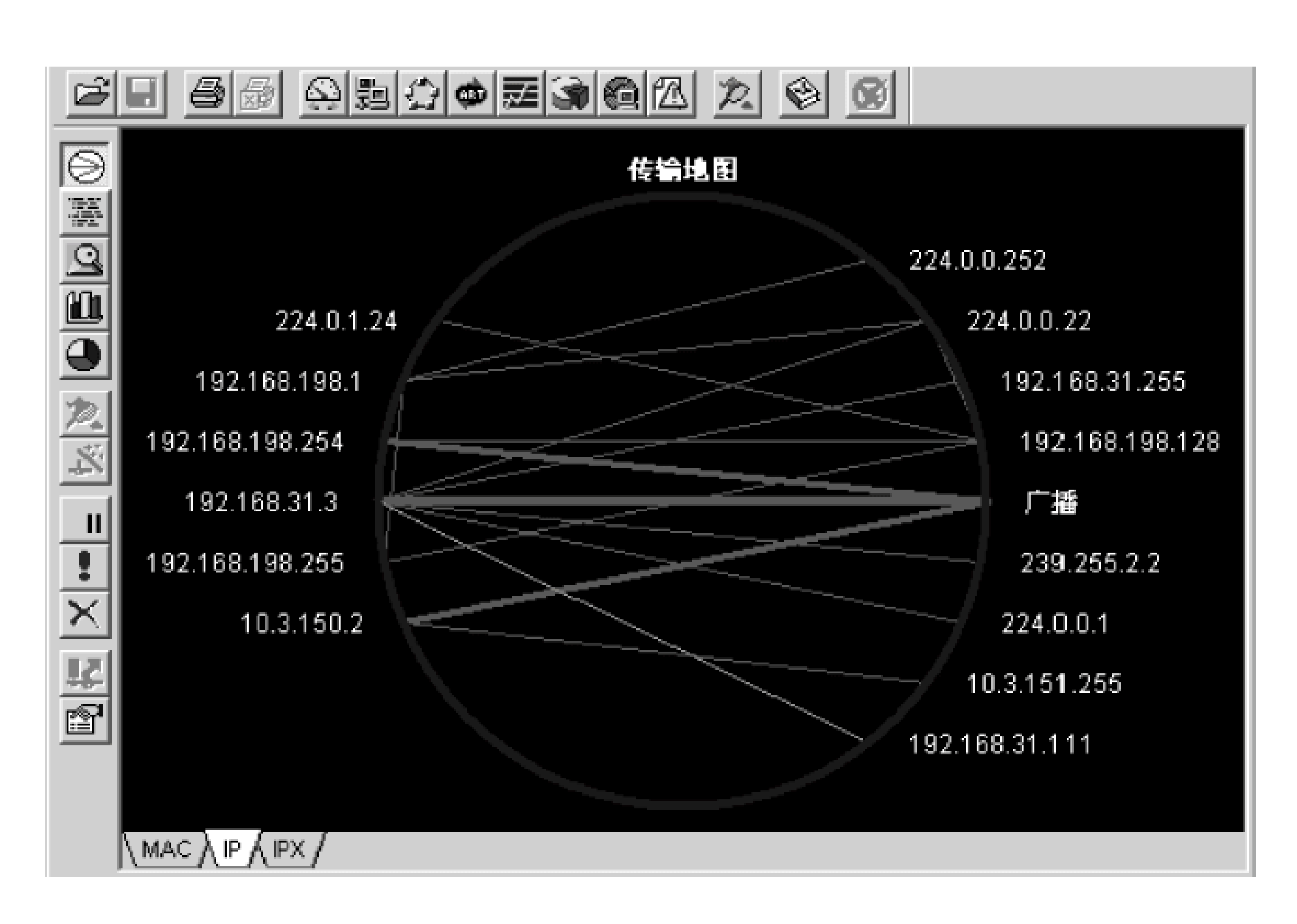


图 4-9　网络连接示意图

有的所有网卡。只要选择需要监听的网卡就可以了。

② 报文捕获功能可以在报文捕获面板中完成。图 4-10 所示是处于开始状态的面板，各个按钮的功能依次是捕获开始、捕获暂停、捕获停止、捕获停止并查看、查看、捕获条件编辑和选择捕获条件。

图 4-10　报文捕获面板

③ 启动 Sniffer Pro 软件，在主窗口的工具栏上单击“捕获设置”按钮，可以对要捕获的协议数据设置捕获过滤条件。默认情况下，捕获所有从指定网卡接收的全部协议数据。捕获到数据后，“停止查看”按钮会由灰色的不可用状态变成彩色的可用状态。

④ 选择“停止查看”按钮会出现如图 4-13 所示窗口，选择最下面的“解码”选项卡，即可查看捕获后的数据的解码。

以捕获计算机 192.168.31.3 所有的数据包为例，操作步骤如下：

① 在主机列表中选择这台计算机，如图 4-11 所示。

② 在窗口左侧单击“捕获”按钮，出现如图 4-12 所示界面。

③ 等到图标变红时，表示已经捕获到数据。单击该图标，弹出如图 4-13 所示界面，选择“解码”选项卡即可看到捕获的所有数据包。

以捕获 Telnet 密码为例，从计算机 192.168.31.111 Telnet 到计算机 192.168.31.3，用

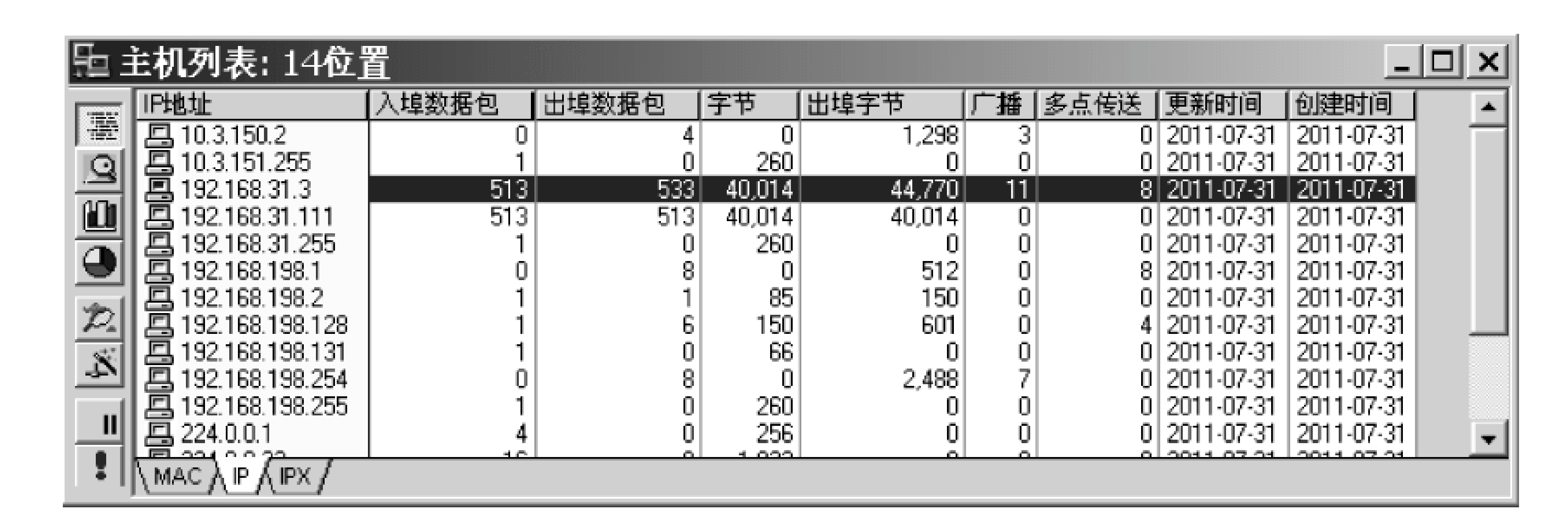


图 4-11 主机列表(2)

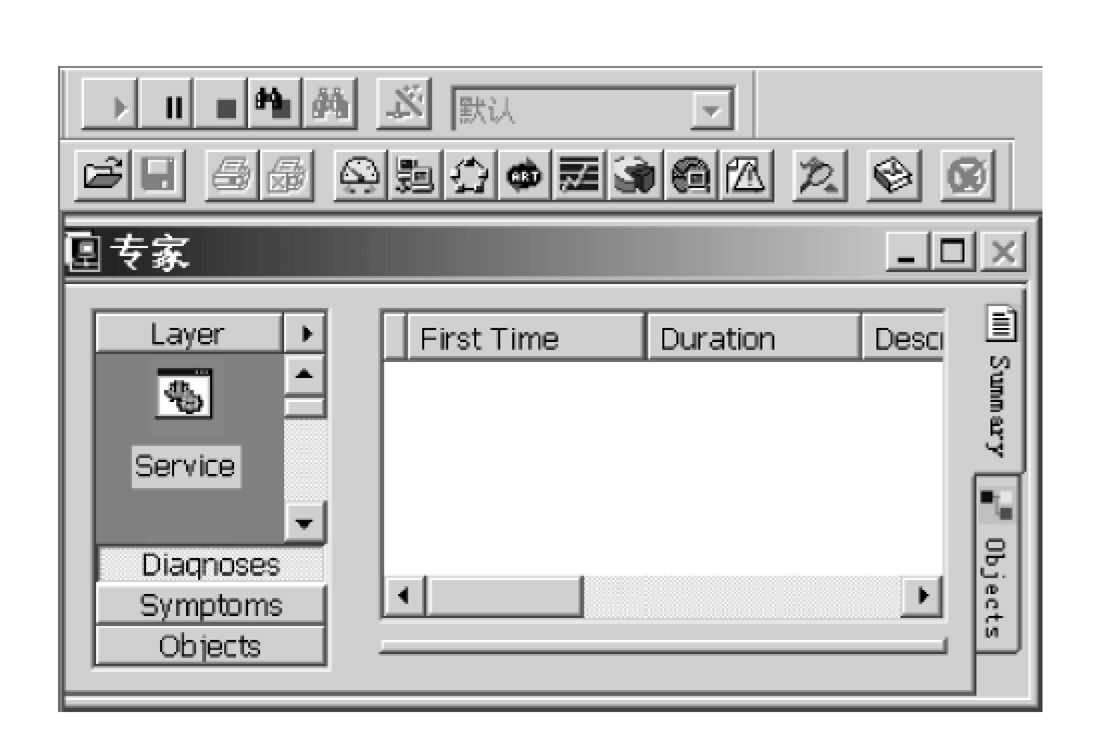


图 4-12 等待捕获数据(1)

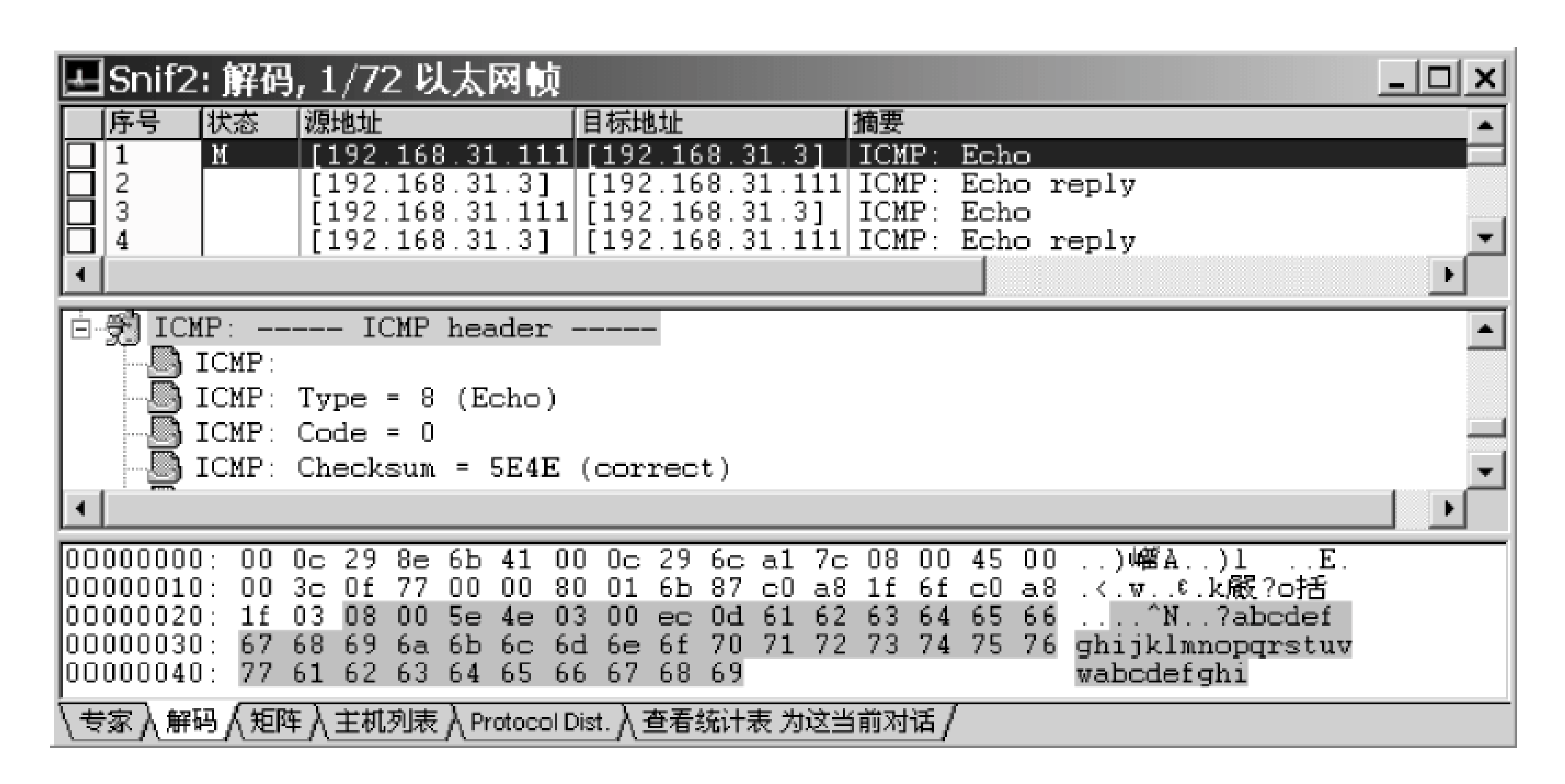


图 4-13 查看捕获到的数据包

Sniffer Pro 捕获到用户名和密码,操作步骤如下:

① 设置规则。选择“捕获”菜单中的“定义过滤器”,然后选择“地址”选项,分别填写两台计算机的 IP 地址,如图 4-14 所示。

② 在“高级”选项中,在“可用到的协议”中选择“IP”→“TCP”→“Telnet”,将“数据包大小”设置为“All”,“数据包类型”设置为“常规”,然后单击“确定”按钮,如图 4-15 所示。

③ 打开 Sniffer Pro 主界面,按 F10 键或者单击工具栏中的黑色小三角开始捕获数据包,将出现等待捕获数据窗口,如图 4-16 所示。

④ 使用管理员账号 administrator 登录被管理计算机 192.168.31.3,密码是 zmczmc,



图 4-14 “地址”选项卡设置(1)



图 4-15 “高级”选项卡设置(1)

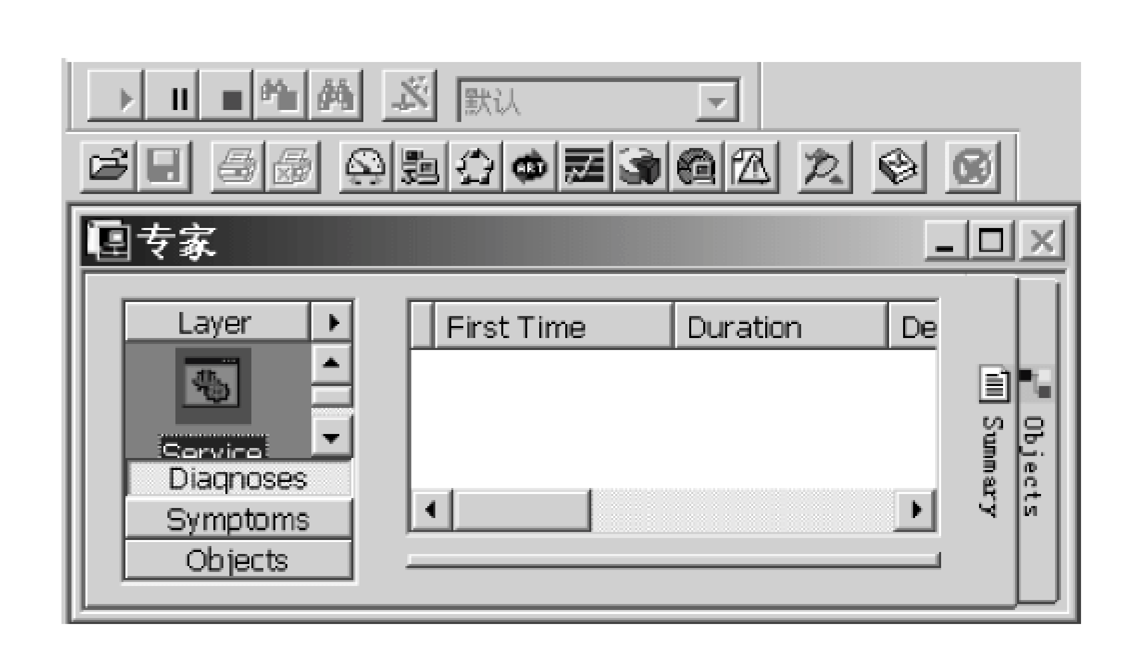


图 4-16 等待捕获数据(2)

运行 telnet 命令,如图 4-17 所示。

⑤ 返回 Sniffer Pro 主界面,看到望远镜图标变红时,表示已捕捉到数据。单击图标查看结果。选择“解码”选项卡可以看到捕获到的所有数据包,可以清楚地看到密码是 zmczmc,如图 4-18 所示。由于账号是双向验证的,所以用户的账号信息会出现重复两次的现象。



图 4-17　远程登录命令(1)

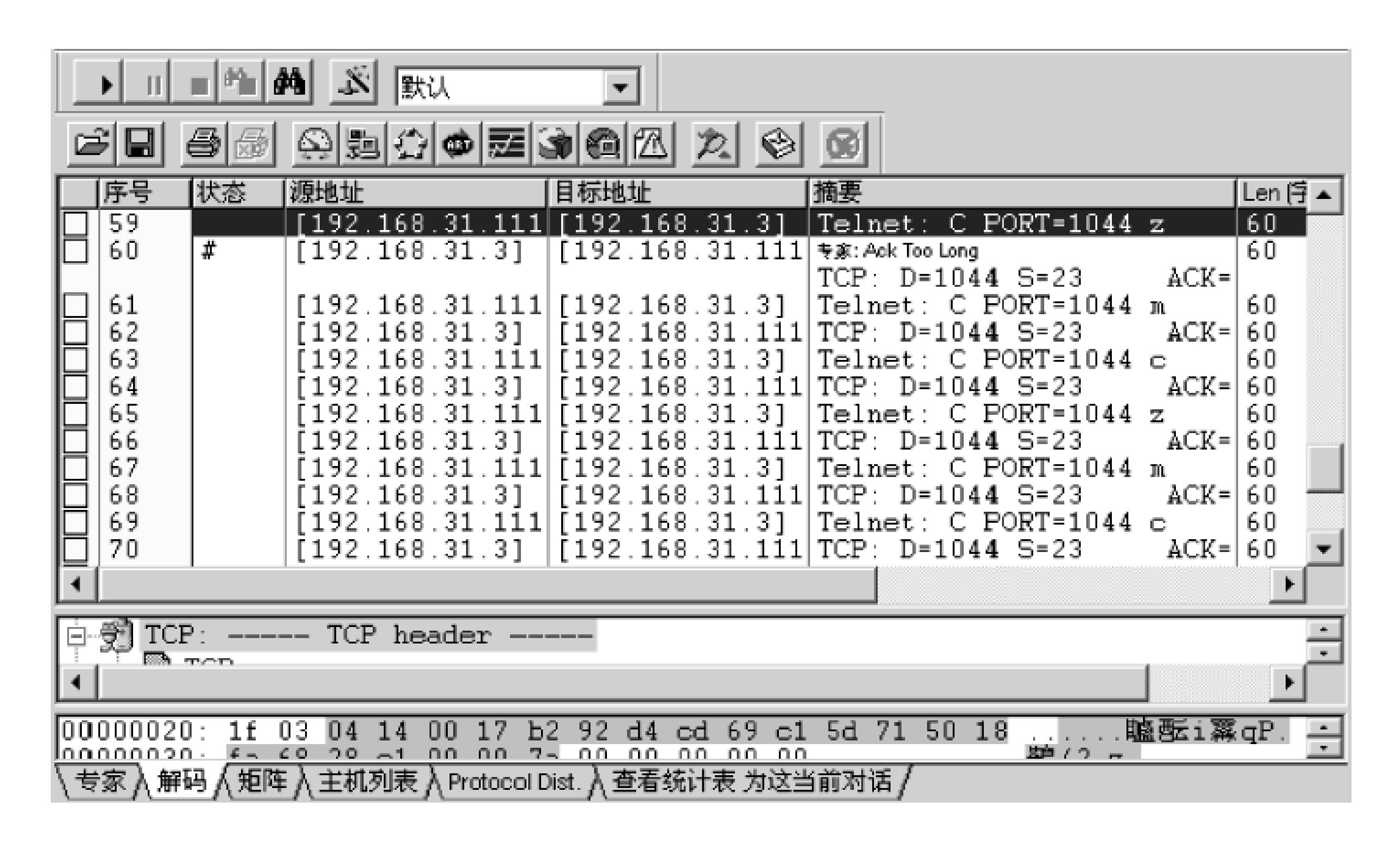


图 4-18　取得密码(1)

以捕获 FTP 密码为例，从计算机 192.168.31.111 FTP 到计算机 192.168.31.3，用 Sniffer Pro 捕获到用户名和密码，操作步骤如下：

① 设置规则。选择“捕获”菜单中的“定义过滤器”，然后选择“地址”选项，分别填写两台计算机的 IP 地址，如图 4-19 所示。

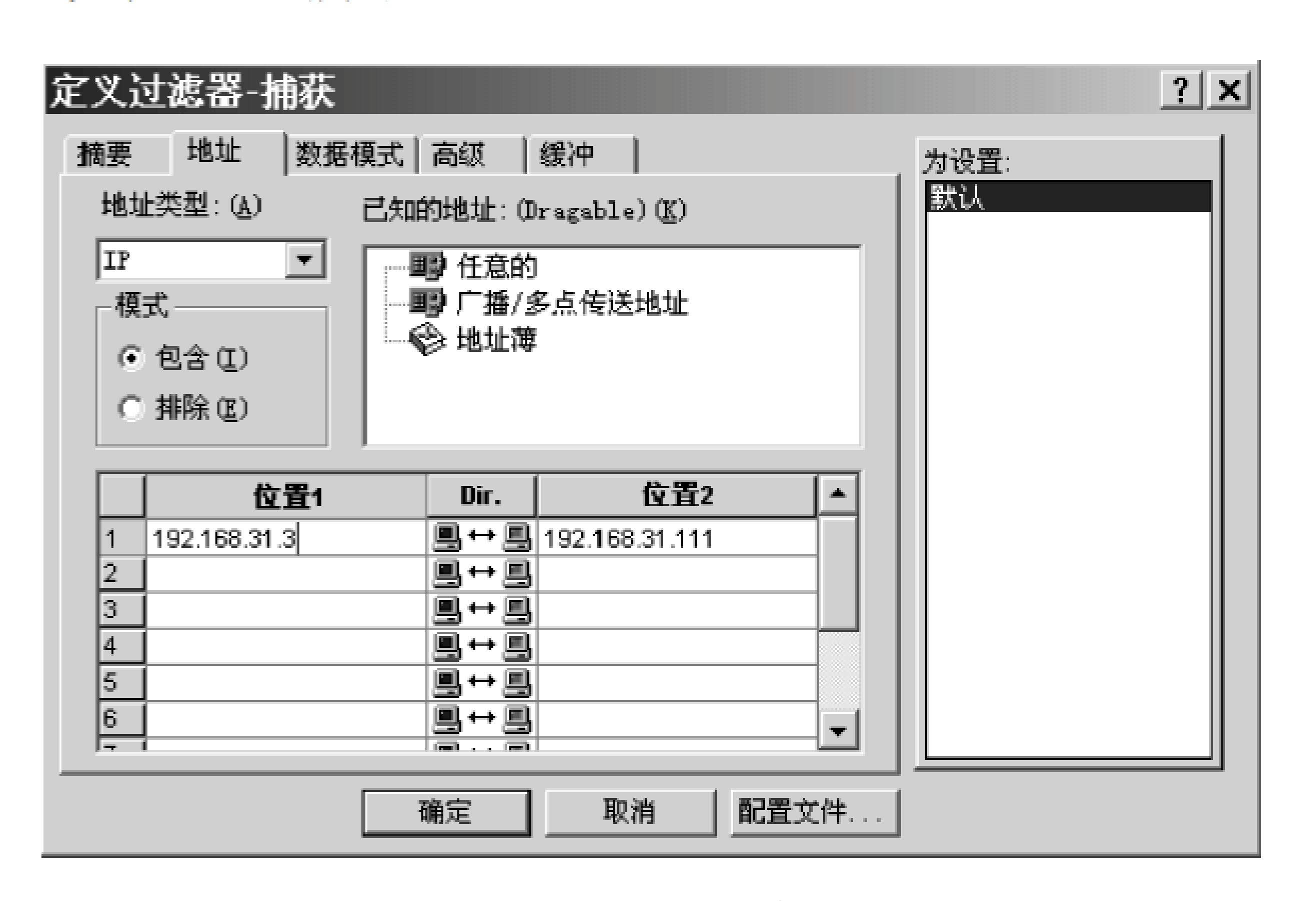


图 4-19　“地址”选项卡设置(2)

② 在“高级”选项中，在“可用到的协议”中选择“IP”→“TCP”→“FTP”，将“数据包大小”设置为“All”，“数据包类型”设置为“常规”，然后单击“确定”按钮，如图 4-20 所示。



图 4-20 “高级”选项卡设置(2)

③ 打开 Sniffer Pro 主界面，按 F10 键或者单击工具栏中的黑色小三角开始捕获数据包，出现等待捕获数据窗口，如图 4-21 所示。

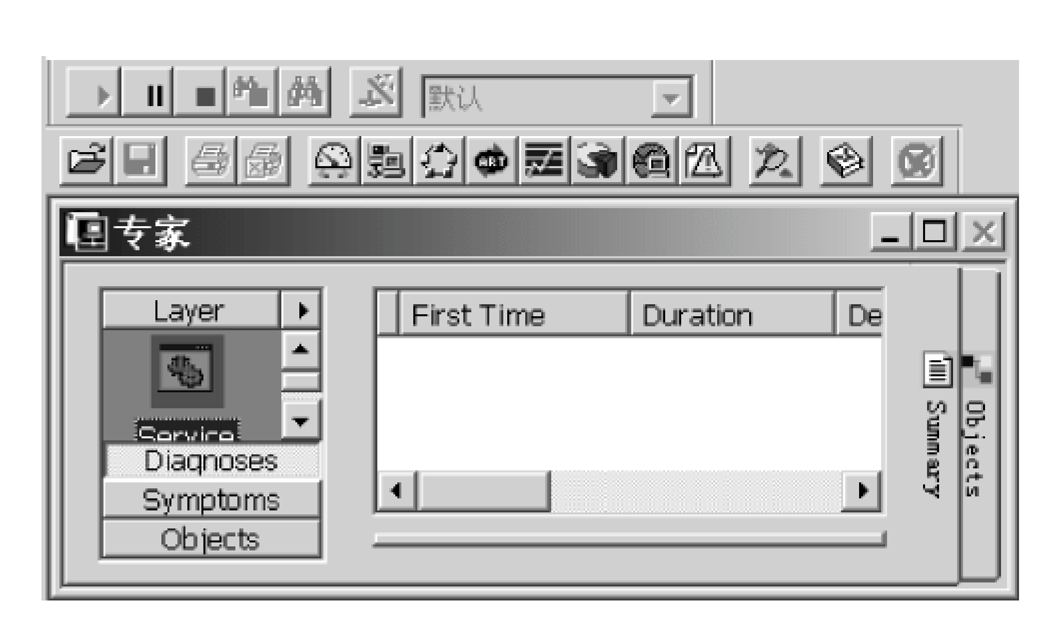


图 4-21 等待捕获数据(3)

④ 运行 FTP 命令 FTP 到一台开有 FTP 服务的计算机 192.168.31.3 上，用户名是 ftp-user，密码是 ftp，如图 4-22 所示。

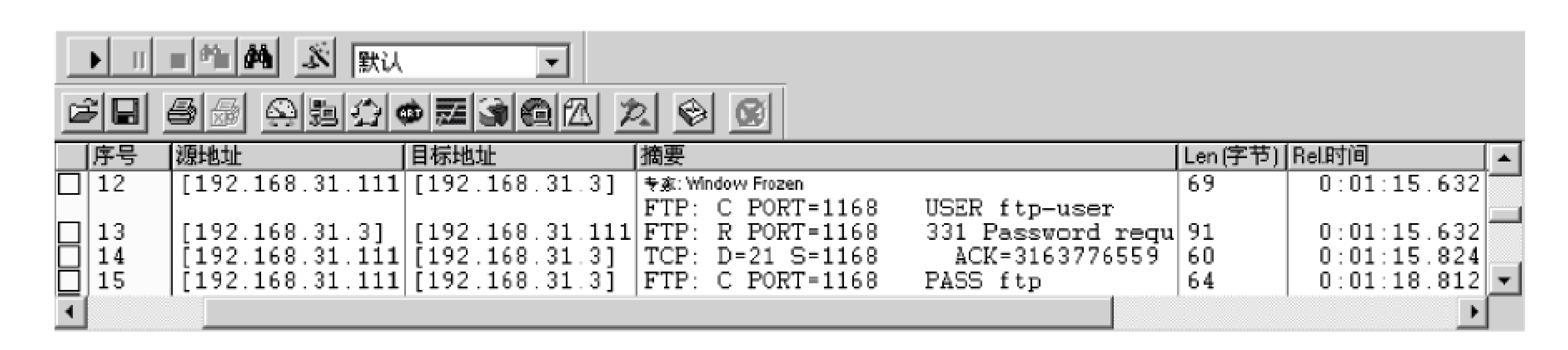
```
命令提示符 - ftp 192.168.31.3
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ftp 192.168.31.3
Connected to 192.168.31.3.
220 Microsoft FTP Service
User (192.168.31.3:(none)): ftp-user
331 Password required for ftp-user.
Password:
230 User ftp-user logged in.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
ftp>
```

图 4-22 远程登录命令(2)

⑤ 返回 Sniffer Pro 主界面，看到望远镜图标变红时，表示已捕捉到数据。单击图标查看结果。选择“解码”选项卡可以看到捕获到的所有包，可以清楚地看到用户名是 ftp -user，密

码是 ftp，如图 4-23 所示。



	序号	源地址	目标地址	摘要	Len(字节)	Rel.时间
□	12	[192.168.31.111	[192.168.31.3]	专家: Window Frozen FTP: C PORT=1168 USER ftp-user	69	0:01:15.632
□	13	[192.168.31.3]	[192.168.31.111	FTP: R PORT=1168 331 Password requ	91	0:01:15.632
□	14	[192.168.31.111	[192.168.31.3]	TCP: D=21 S=1168 ACK=3163776559	60	0:01:15.824
□	15	[192.168.31.111	[192.168.31.3]	FTP: C PORT=1168 PASS ftp	64	0:01:18.812

图 4-23　取得密码(2)

4.4.2　任务 2：Wireshark 工具的使用

1. 任务目标

掌握 Wireshark 的安装方法，熟练掌握使用 Wireshark 分析数据包的 3 个步骤：选择数据包→分析协议→分析数据包内容，并能使用 Wireshark 嗅探一个 FTP 过程。

2. 工作任务

(1) 设置 Wireshark 的过滤规则；

(2) 指定过滤器；

(3) 用 Wireshark 捕获数据包。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机，通过网络相连。

(2) 软件工具：Wireshark 工具。

4. 实施过程

使用 Wireshark 时最常见的问题是当用户使用默认设置时，会得到大量冗余信息，以至于很难找到需要的部分。

(1) 设置 Wireshark 的过滤规则

在用 Wireshark 截获数据包之前，应该为其设置相应的过滤规则，可以只捕获感兴趣的数据包。要为 Wireshark 配置过滤规则，首先在 Wireshark 的主界面选择“Capture”→“Capture Filter”菜单项，打开“Wireshark：Capture Filter”对话框。对话框右侧的列表框中列出了已经存在的过滤器，单击任意一个，可以在对话框的下侧看到该过滤器的名称和过滤规则。可以通过对话框左侧的“New”和“Delete”按钮在对话框中添加或删除过滤器。在 Wireshark 中添加过滤器时，需要为其指定名字及规则。

例如，要在主机 192.168.5.2 和 192.168.5.4 之间建立过滤器，可以在“Filter name”编辑框内输入过滤器名字“1”，在“Filter string”编辑框内输入过滤规则“host 192.168.5.2 and 192.168.5.4”，然后单击“New”按钮，如图 4-24 所示。

下面举例说明几种常见的过滤条件。

① host 192.168.0.1：程序只捕获 IP 地址为 192.168.0.1 的数据包；

② tcp：只捕获 TCP 数据包；

③ port 80：捕获 TCP 或 UDP 协议且端口为 80 的数据包；

④ not tcp port 3389：不捕获 TCP 端口为 3389 的数据包；

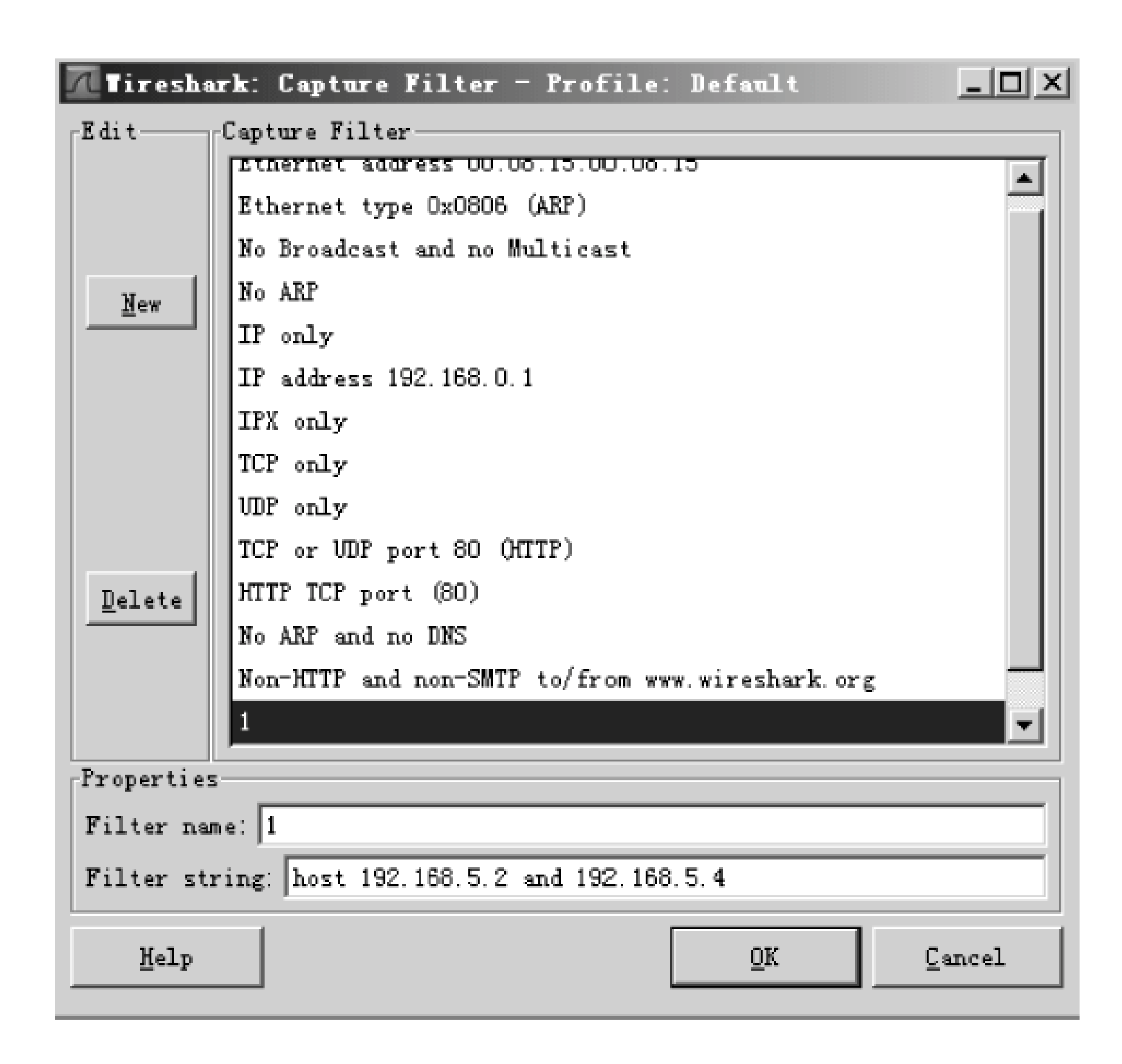


图 4-24　为 Wireshark 添加一个过滤器“1”

⑤ src 192.168.0.1 and dst 192.168.0.2：捕获源地址为 192.168.0.1 且目标地址为 192.168.0.2 的数据包。

（2）指定过滤器

Wireshark 能够同时维护多个过滤器，网络管理员可以根据实际需要选用不同的过滤器，这在很多情况下是非常有用的。例如，一个过滤器可能用于截获两台主机间的数据包，而另一个可能用于截获 ICMP 包来诊断网络故障。具体操作步骤如下：

① 在 Wireshark 主界面单击查看本机网卡状态配置按钮“Interface List”，如图 4-25 所示。

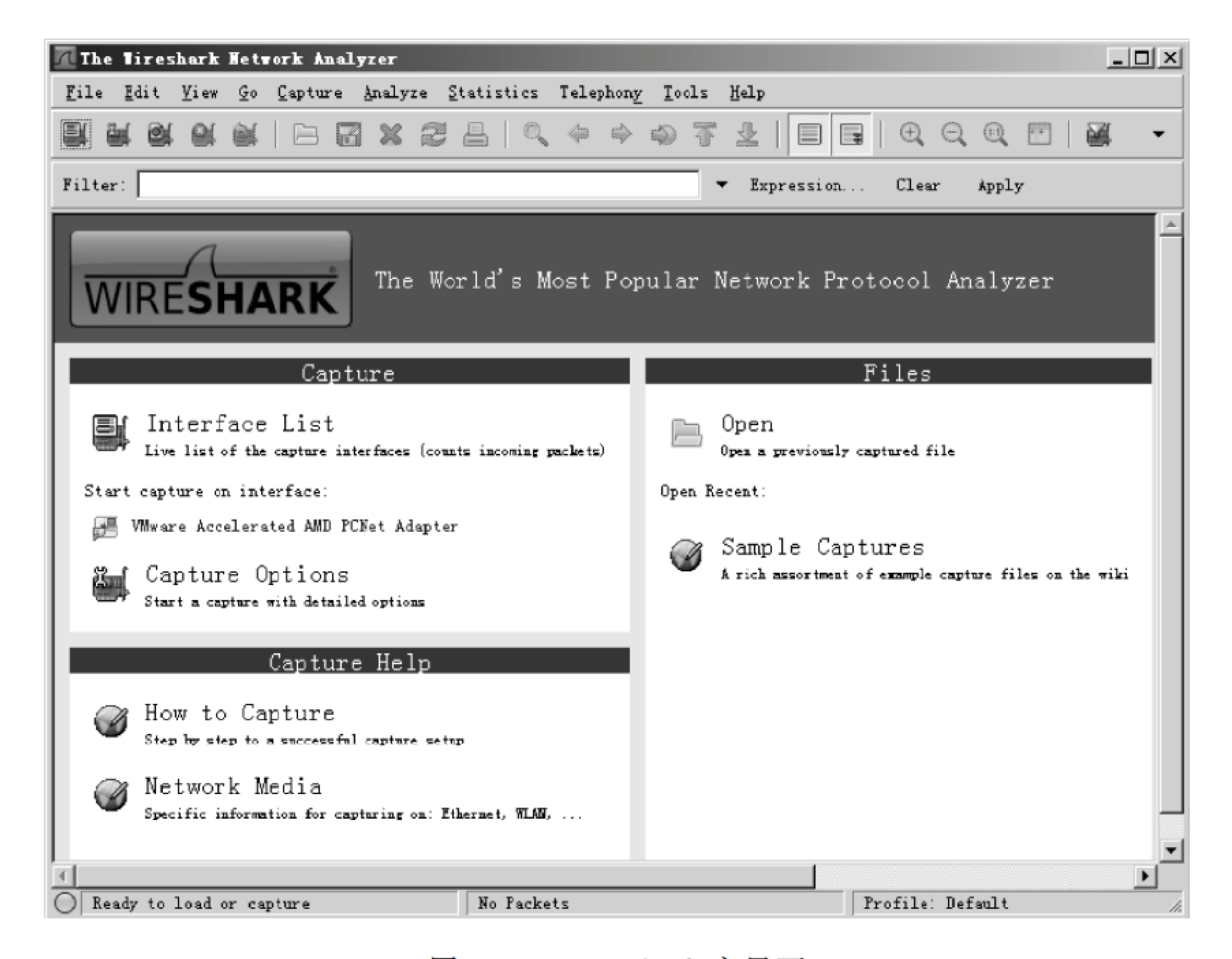


图 4-25　Wireshark 主界面

② 弹出“Wireshark：Capture Interfaces”对话框，从中可以看出本机的网卡信息。“Description”是可以选择的网卡名称，“IP”是对应网卡的 IP 地址。单击“Options”按钮，如图 4-26 所示。

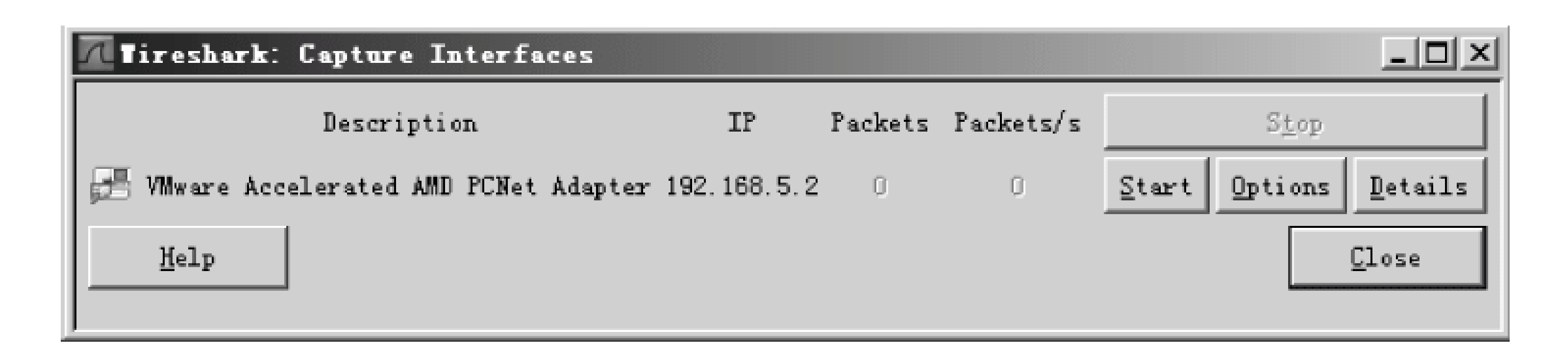


图 4-26　为 Wireshark 指定网络接口

③ 打开“Capture Options”对话框，然后单击“Capture Filter”按钮，在对话框右侧的列表框中选择过滤器“1”。单击“OK”按钮后，回到“Capture Options”对话框主界面，可以看到“Capture Filter”变成了“host 192.168.5.2 and 192.168.5.4”，如图 4-27 所示。

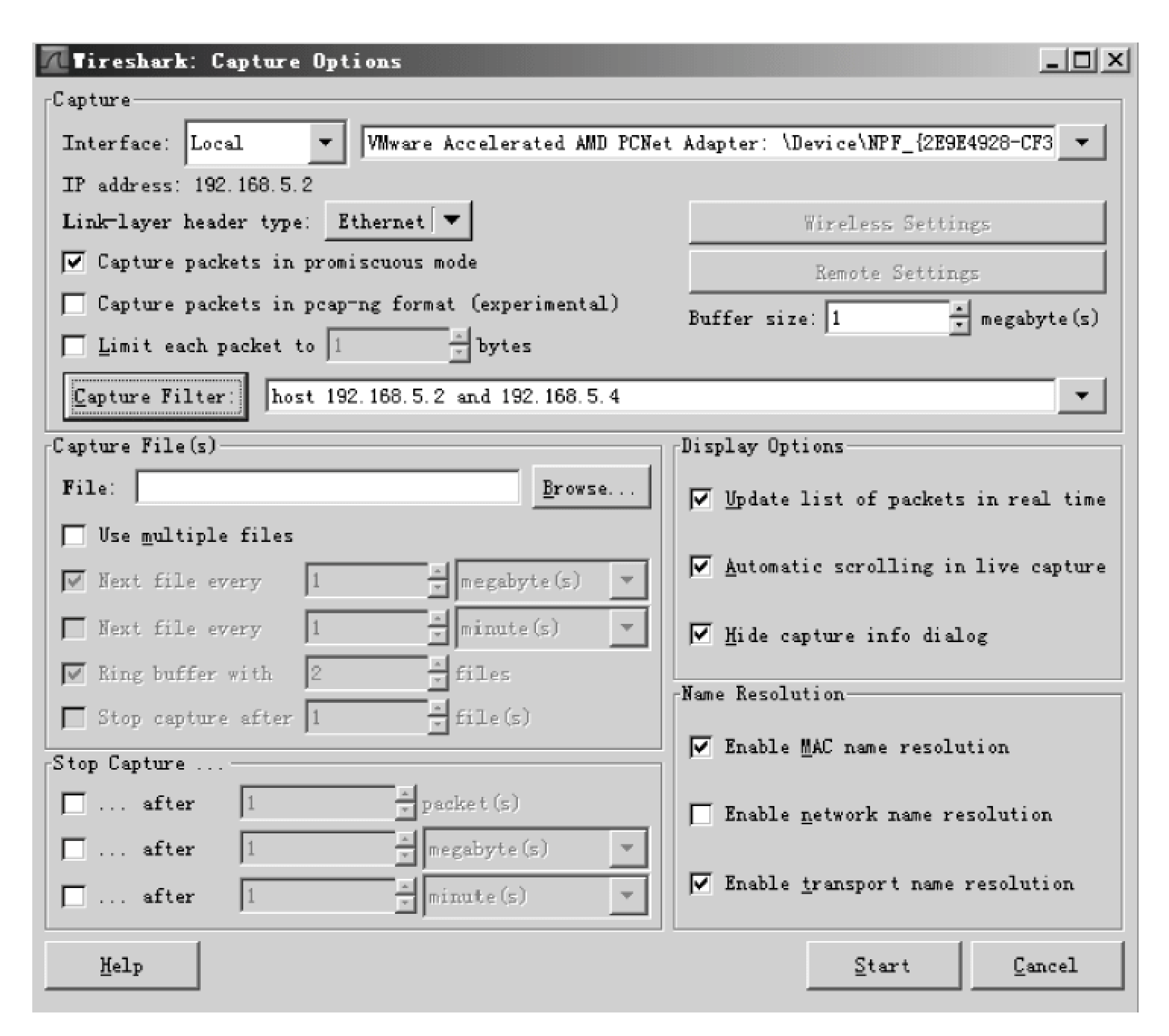


图 4-27　“Capture Options”对话框设置

④ 单击“Start”按钮，即开始捕获主机 192.168.5.2 和 192.168.5.4 之间的数据包。

“Capture Options”其他选项的含义分别如下：

① Interface(接口)：该字段指定在哪个网络接口(网卡)进行捕获。这是一个下拉字段，只能从下拉列表中选择 Wireshark 识别出来的接口。默认是第一张支持捕获的非 loopback 接口卡。这里选择本地(Local)网卡。实验环境不同，可能使用不同的网卡。

② IP address(IP 地址)：所选接口卡的 IP 地址。如果不能解析出 IP 地址，显示“unknown”。

③ Link-layer header type(链路层头类型)：大多数保持默认值。

④ Buffer size n megabyte(s)(缓冲区大小：n 兆)：输入捕获时使用的缓冲区的大小。

这是核心缓冲区的大小,捕获的数据首先保存在这里,直到写入磁盘。如果遇到包丢失的情况,增加这个值可能解决问题。

⑤ Capture packets in promiscuous mode(在混杂模式捕获包):该选项允许是否将网卡设置在混杂模式。如果不指定,Wireshark 仅仅捕获那些进入本地计算机发送或接收到的数据包,而不是局域网网段上所有的包。

⑥ Limit each packet to n bytes(限制每一个包为 n 字节):该字段设置每一个数据包的最大捕获数据量。Disable 选项默认是 65535,对于大多数协议来讲够了。

(3) 用 Wireshark 捕获数据包

单击窗口中的“Start”按钮,会出现所捕获数据包的统计。想停止时,单击“Capture”菜单中的“Stop”按钮。

例如,当主机 192.168.5.2 在命令行窗口 ping 主机 192.168.5.4 时,会出现如图 4-28 所示的捕获信息。

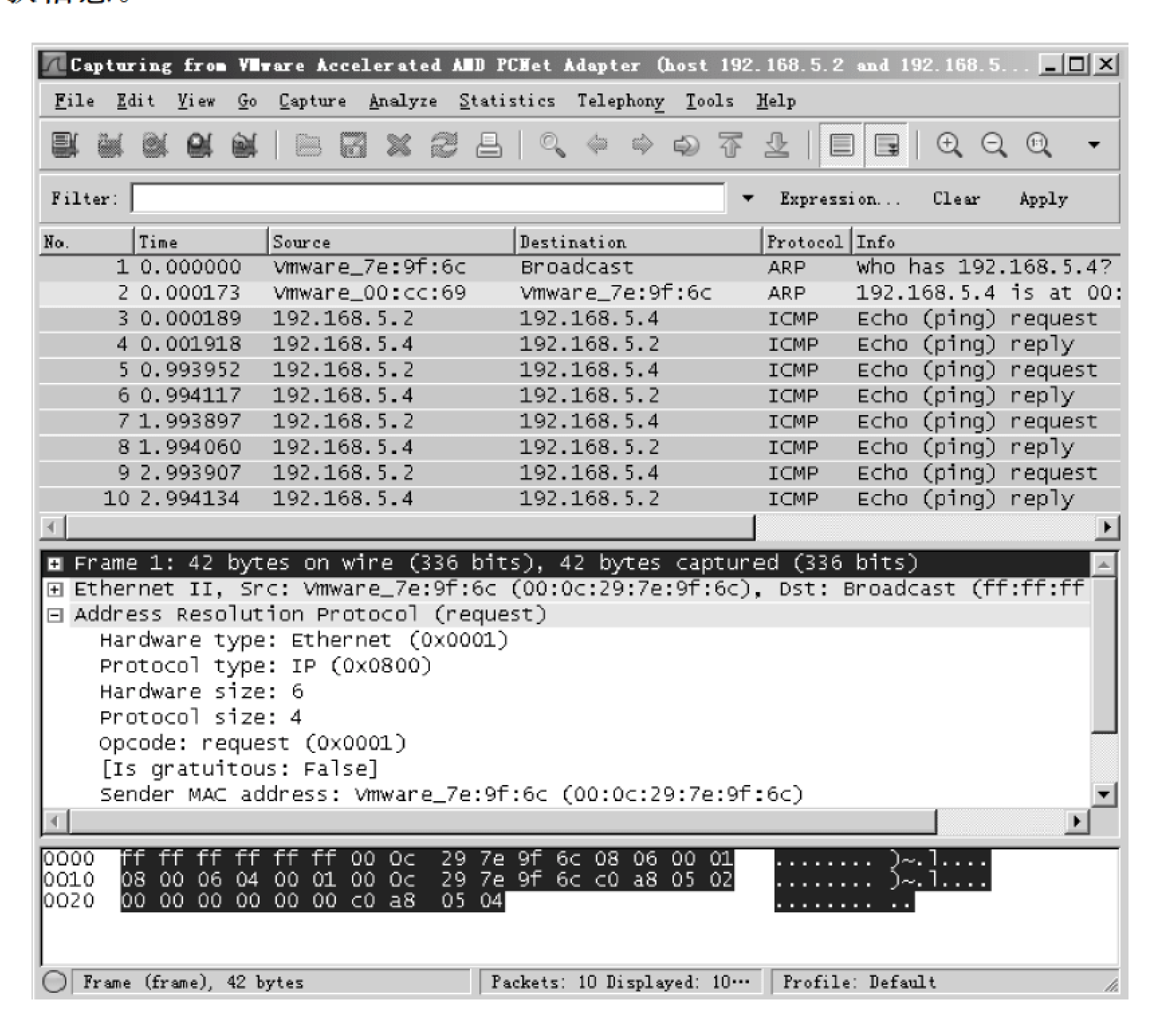


图 4-28 Wireshark 分析数据包

Wireshark 和其他图形化嗅探器使用基本类似的界面,整个窗口分为 3 个部分:最上面为数据包列表,用来显示截获的每个数据包的总结性信息;中间为协议树,用来显示选定的数据包所属的协议信息;最下面是以十六进制形式表示的数据包内容,用来显示数据包在物理层上传输时的最终形式。使用 Wireshark 可以很方便地对截获的数据包进行分析,包括该数据包的源地址、目标地址、所属协议等。

图 4-28 所示是在 Wireshark 中对一个 HTTP 数据包进行分析时的情形。图中最上边的数据包列表中显示了被截获的数据包的基本信息。

中间是协议树，通过协议树可以得到被截获的数据包的更多信息，如主机的 MAC 地址、IP 地址、TCP 端口号，以及 HTTP 协议的具体内容。通过扩展协议树中的相应节点，可以得到该数据包中携带的更详尽的信息。

最下面是以十六进制显示的数据包的具体内容，这是被截获的数据包在物理媒体上传输时的最终形式。当在协议树中选中某行时，与其对应的十六进制代码同时被选中，可以很方便地对各种协议的数据包进行分析。

下面举例说明用 Wireshark 嗅探一个 FTP 的过程。

由于 FTP 中的数据都是明文传输的，所以很容易获得。

① 打开 Wireshark 开始捕获数据。

② 登录 FTP 服务器，如图 4-29 所示。

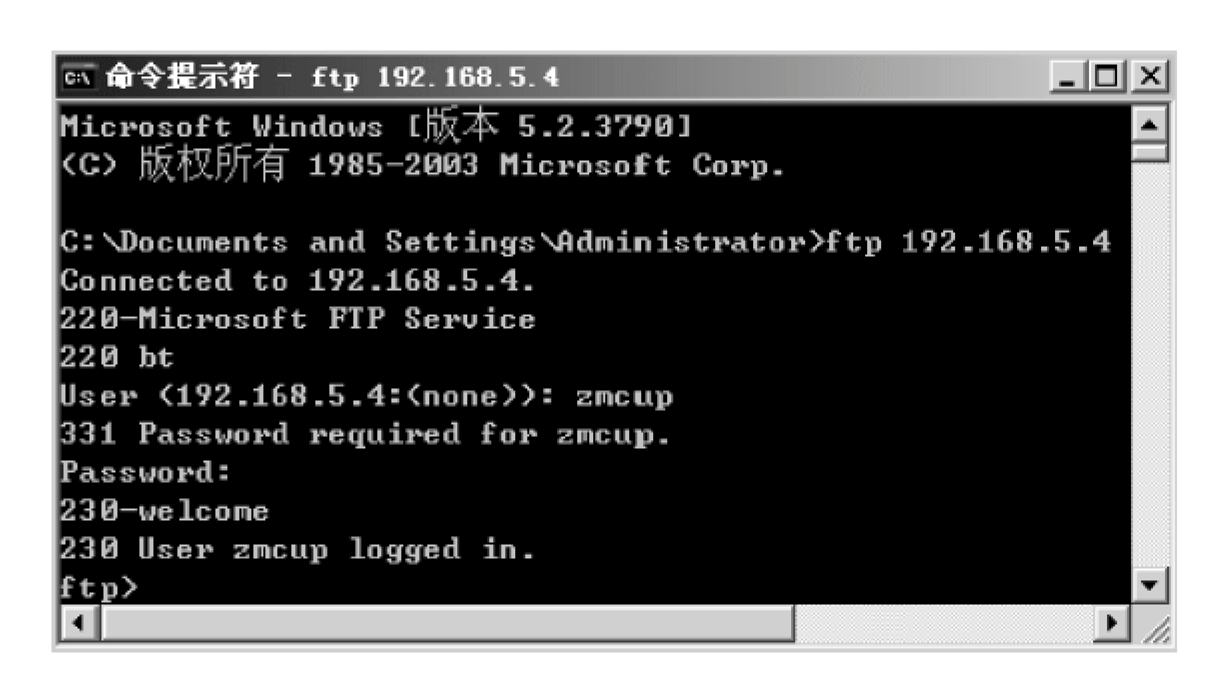


图 4-29　FTP 服务器登录过程

③ 登录后，Wireshark 停止捕获数据，可以在 Wireshark 中看到分析结果。登录的用户名是 zmcup，密码是 zmc，如图 4-30 所示。

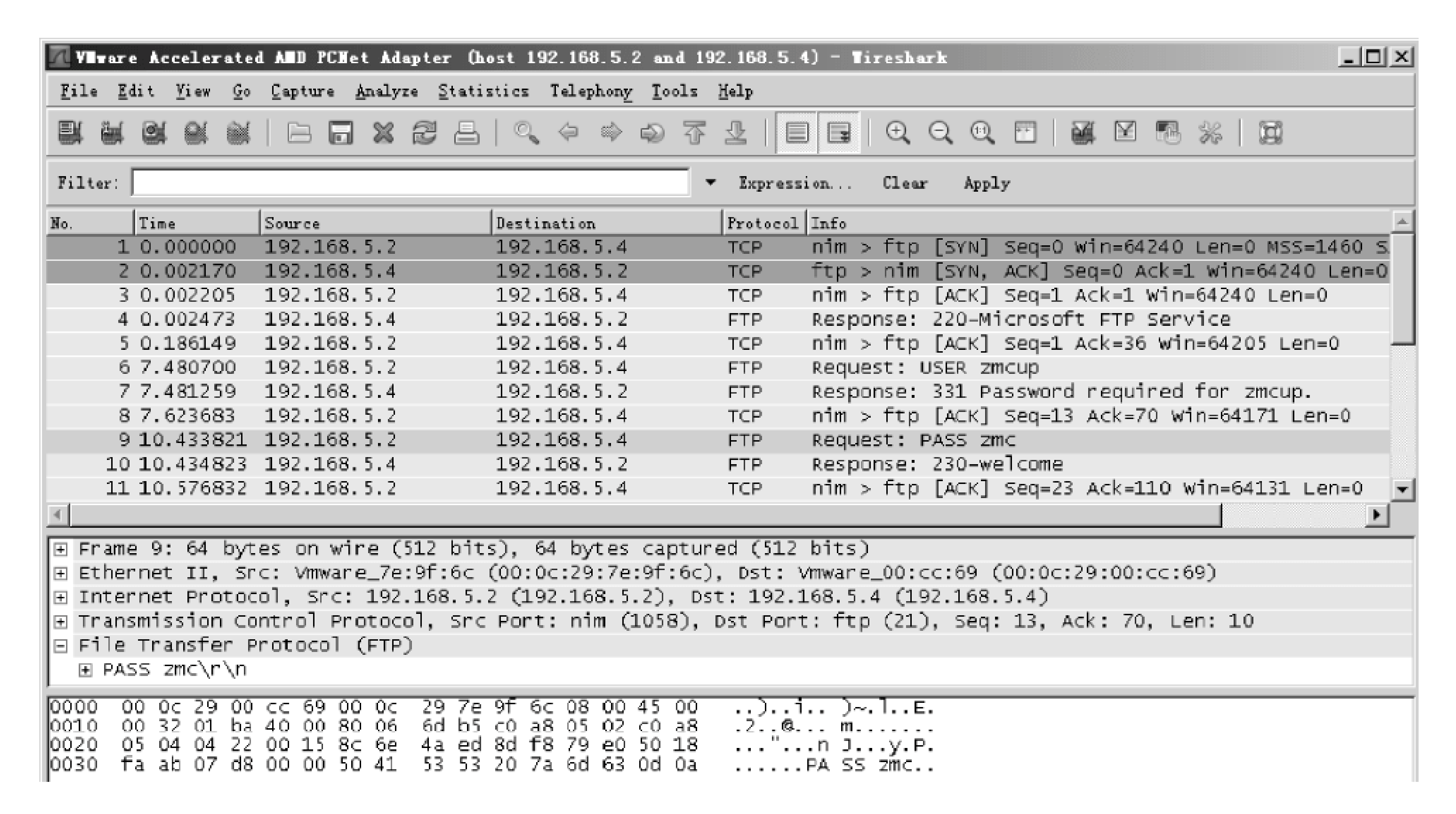


图 4-30　FTP 登录结果

通过这样的方法，可以掌握 FTP 的工作过程。

4.5 常见问题解答

1. 在 TCP/IP 协议中，数据的传输单位是什么？测试网络速度的常用单位是什么？

答：在 TCP/IP 协议中，数据被分成若干个包(packets)进行传输，包的大小跟操作系统、网络带宽有关，一般为 64、128、256、512、1024 等，包的单位是字节。网络速度通常用 Kb/s、KB、Mb/s 来表示，B 和 b 分别代表 Byte(字节)和 bit(比特)，1 比特就是 0 或 1。1B=8b。1Mb/s(兆比特每秒)=1×1024/8=128(KB/s，字节每秒)。例如，常见的 ADSL 下行 512K 指的是每秒传输 512K 比特(Kb)，也就是每秒 512K/8=64K 字节(KB)。

2. 系统没有 Telnet 服务怎么办？

答：在任务栏上单击"开始"→"运行"，在"运行"对话框中输入"tlnsvr /service"，启动 Telnet 服务。

4.6 过关练习

一、选择题

1. 网络监听是(　　)。
   A. 远程观察一个用户的计算机　　B. 监视网络的状态、传输的数据流
   C. 监视 PC 系统的运行情况　　D. 监视一个网站的发展方向
2. 下面关于几个网络管理工具的描述中，错误的是(　　)。
   A. netstat 可用于显示 IP、TCP、UDP、ICMP 等协议的统计数据
   B. Sniffer 能够使网络接口处于杂收模式，从而可接收网络上传输的分组
   C. winipcfg 采用 MS-DOS 工作方式显示网络适配器和主机的有关信息
   D. tracert 可以发现数据包到达目标主机所经过的路由器和到达时间
3. 嗅探器可以使网络接口处于杂收模式，在这种模式下，网络接口(　　)。
   A. 只能够响应与本地网络接口硬件地址相匹配的数据帧
   B. 只能够响应本网段的广播数据帧
   C. 只能够响应组播信息
   D. 能够响应流经网络接口的所有数据帧

二、简答题

1. 常用的网络监听工具有哪些？
2. 网络嗅探器的工作原理是什么？

三、操作题

利用嗅探工具嗅探 Telnet 远程登录密码。

工作任务五

远程控制

5.1 用户需求与分析

远程控制本来用于专家的远程协助，解决计算机系统中的问题，但该技术被黑客运用后，就变成了攻击他人计算机系统的一种手段。通过远程控制技术，黑客可以获取远程计算机的许多重要信息，例如个人账号和密码等。通过对远程计算机的完全控制，对其中的所有文件进行操作、修改注册表、监视屏幕操作的一举一动，甚至可以实时控制远程计算机用户的操作，例如锁定键盘、远程关机等，就像在操作自己的计算机一样。

5.2 预备知识

5.2.1 远程控制的原理

远程控制就是利用远程控制软件在两台计算机之间建立起一条数据交换的通道，使主控端可以向被控端发送指令，操纵被控端完成某些特定的工作。要实现远程控制，需要满足一些条件：首先，主控计算机和被控计算机都处在网络中；其次，双方有相同的通信协议，一般使用 TCP/IP 协议进行通信；最后，在两台计算机上都必须安装远程控制软件，而且一台必须配置成被控端，另一台必须配置成主控端。被控端计算机等候与主控端计算机连接，而且被控端由主控端控制，控制被控端计算机中的各种应用程序运行。主控端负责发送指令和显示远程被控端计算机执行程序的结果，而运行程序所需要的系统资源都由被控端计算机负责。

5.2.2 认识木马

木马是目前最主要的网络安全威胁之一。木马的全名叫“特洛伊木马”，来源于希腊神话“木马屠城记”。据《荷马史诗》中描述，希腊皇后海伦被英俊潇洒的特洛伊王子巴德里诱骗回国后，希腊国王“冲冠一怒为红颜”，派兵攻打特洛伊城，只因城池坚固，花了 10 年时间始终无果。后有谋士献计制作一匹空心大木马，内藏勇士，故意佯装失败留下木马。特洛伊人果然上当，把木马作为战利品拉入城中大摆庆功宴。深夜，木马中的勇士趁特洛伊人酒醉沉睡之际，打开城门里应外合，一举攻陷了特洛伊城。

木马是一种基于 C/S(客户端/服务器)模式的远程控制程序，具有隐蔽性、非授权性、自动运行性等特点。隐蔽性是指木马程序隐藏于服务器端，即使计算机用户发现计算机感染

了木马，也很难确定木马的位置。这也是木马程序与一般远程控制软件最大的区别。非授权性是指控制端和服务器端建立连接后，控制端就拥有了服务器端的大部分操作权限，包括修改和删除文件、修改注册表、控制键盘和鼠标等操作权限。自动运行性是指当系统启动时木马程序自动运行，它通常依附在系统的启动配置文件中，例如 win.ini、system.ini、winstart.bat 以及启动组文件中。

完整的木马系统包括硬件、软件和网络连接 3 部分。硬件包括服务器端和控制端。服务器端是被黑客安装木马服务程序的目标计算机，即被远程控制的一方；控制端是黑客实施远程攻击的一方，即远程控制服务器端的一方。网络连接是服务器端和控制端之间的通信通道，为服务器端发送获取的信息，为控制端发送控制命令提供渠道。

木马的伪装方式主要包括修改图标、捆绑文件、出错提示、定制端口、自我销毁、自动更名。有些木马把服务器端程序的图标改成 jpg、txt、zip、html 等文件的形式，具有很强的迷惑性；有些木马把自己捆绑在安装程序或可执行文件 exe、com、bat 上，程序运行时木马服务器端也开始运行；有些木马具有出错显示功能，当木马服务器端用户打开木马程序时，会弹出一个错误提示框。老式木马端口都是固定的，新式木马端口可以自定义，控制端用户可以指定 1024～65535 之间的任一端口作为木马端口。当木马在服务器端安装成功后，原木马文件自动销毁，服务器端用户就很难找到木马的来源。目前，很多木马程序可以由控制端用户命名，给木马的查找带来了困难。

5.2.3 木马的发展与分类

木马程序技术发展至今经历了四代：第一代伪装型病毒、第二代 AIDS 型木马、第三代网络传播型木马和第四代隐形木马。第一代木马不具备传染性，它通过伪装成一个合法程序诱骗用户上当。第二代木马通过电子邮件进行传播。第三代木马增加了“后门”功能和键盘记录功能，具有伪装和传播两种特点。第四代木马采用插入内核的潜入方式，利用远程插入线程、嵌入 DLL 线程等技术实现程序隐藏，利用反弹端口技术突破防火墙限制，使被侵用户毫无察觉。

按照木马的特性，可以把木马分为破坏型、密码发送型、键盘记录型、DoS 攻击型、反弹端口型、代理型和远程访问型等。破坏型木马破坏并删除文件，能自动删除目标主机上的 dll、ini、exe 文件，一旦感染，将严重威胁计算机的安全。密码发送型木马能找到目标主机的隐藏密码，并把它发送到指定邮箱。Windows 提供的密码记忆功能使用户不必每次都输入账号和密码，这类木马就是利用这一点获取目标主机的密码，大多数使用 25 号端口发送邮件，在系统启动时重新运行。键盘记录型木马记录目标主机在在线和离线状态下敲击键盘的情况，并存储在 log 文件中，发送到指定邮箱，黑客通过分析键盘记录获得密码、信用卡账号等有用信息。DoS 攻击型木马的危害不是体现在被感染的目标主机上，而是体现在黑客利用它来攻击其他计算机，给网络和服务造成很大的伤害。一种类似的 DoS 攻击型木马叫做邮件炸弹木马，目标主机一旦感染，会生成各种各样主题的邮件，向特定邮箱不停发送邮件，直到对方瘫痪，不能接收邮件为止。与一般的木马相反，反弹端口型木马的被控制端使用主动端口，控制端使用被动端口，因为防火墙对于进入的链接进行严格过滤，对于出去的链接疏于防范。控制端的被动端口通常设为 80，即使目标主机用户检查自己端口时发现 80 端口打开，也可能以为是自己在浏览网页导致的结果。代理型木马是黑客发动攻击的跳

板，在入侵的同时掩盖自己的踪迹。通过代理型木马，黑客可以匿名使用 Telnet 等程序，掩饰自己的身份。远程访问型木马是目前使用最广泛的木马，是一种基于远程控制的工具，能远程访问目标主机的硬盘。

5.2.4 常见远程控制工具介绍

下面介绍几种最常见的远程控制软件。

1. 单点远程控制软件 pcAnywhere

pcAnywhere 是由 Symantec（赛门铁克）公司出品的远程控制软件，可在 Windows XP/2003 平台上运行。它功能强大，支持几乎所有的网络连接方式与网络协议。利用它，网络管理人员可以轻松实现在本地计算机上控制远程计算机，使得两地的计算机可以协同工作。

pcAnywhere 的工作原理是首先由主控端向被控端发送远程控制请求，控制端接收到请求后给出响应信号，要求对主控端的合法身份进行验证。此时，主控端必须向被控端提供远程控制所需要的合法登录名和密码。如果被控端验证账号和密码正确，则主控端可以开始远程控制被控端进行操作；否则，被控端会拒绝主控端的控制请求。被控端利用身份验证来确保自身安全，还可以决定哪些用户能够连接，以及用户所具有的权限是什么。

2. 多点远程控制软件 QuickIP

对网络管理来说，一台主机要管理多台计算机，需要应用到多点远程控制技术。QuickIP 就是一款具有多点远程控制技术的工具。QuickIP 是基于 TCP/IP 的计算机远程控制软件，使用 QuickIP 可以通过局域网或互联网全权控制远程的计算机。服务器可以同时被多台客户机控制，一台客户机也可以同时控制多台服务器。

QuickIP 具有 FTP 功能，可以上传、下载远程文件，以树状展示远程计算机所有磁盘驱动器的内容；可以对远程屏幕进行录像；可以控制远程主机的鼠标、键盘，就像操作本地计算机一样；可以控制远程的录音设备，具有网络电话功能；可以控制远程计算机的所有进程、窗口、程序，控制远程主机重新启动、关机、登录等。QuickIP 具有安全的密码验证，客户机必须知道服务器密码才能进行控制；网络数据采用压缩传输，因此数据传输速度快并且很安全。QuickIP 具有定位功能，在不知道远程主机 IP 地址或域名的情况下，能迅速连接到远程主机上；可用于服务器管理、远程资源共享、网吧机器管理、远程办公、远程教育、排除故障、远程监控等。QuickIP 可运行在 Windows XP/2003 等系统上。由于 QuickIP 将服务器端和客户端合并在一起，所以每台计算机中都要安装服务器端和客户端，这样，安装了 QuickIP 的网络计算机都可以作为客户端控制其他计算机，也可以被其他计算机控制。

3. 木马工具“任我行”软件

“任我行”是一款功能强大的远程控制软件，它的功能仅次于“灰鸽子”远程控制软件，不同的是“任我行”软件提供了两种不同的配置类型，更易于管理。黑客经常利用这款软件来监控目标主机。

5.3 方案设计

方案设计如表 5-1 所示。

表 5-1 方案设计

任务名称	远程控制
任务分解	1. 使用 pcAnywhere 远程控制计算机 (1) 被控端的配置 (2) 主控端的配置 (3) 远程控制的实现 2. 使用 QuickIP 对多点计算机进行远程控制 (1) 设置 QuickIP 服务器密码 (2) 登录客户端 (3) 查看 QuickIP 服务器信息 3. 使用"任我行"软件对远程计算机进行控制 (1) 配置正向连接型服务端 (2) 配置反向连接型服务端 (3) 通过服务端程序进行远程控制
能力目标	1. 能配置 pcAnywhere 的被控端 2. 能配置 pcAnywhere 的主控端 3. 能使用 pcAnywhere 实现远程控制 4. 能设置 QuickIP 服务器密码 5. 能登录 QuickIP 客户端 6. 能查看 QuickIP 服务器信息 7. 能配置"任我行"软件的正向连接型服务端 8. 能配置"任我行"软件的反向连接型服务端 9. 能通过"任我行"软件的服务端程序进行远程控制
知识目标	1. 了解远程控制的原理 2. 了解木马的来源 3. 熟悉木马程序的特点 4. 熟悉木马的伪装方式 5. 了解木马系统的组成 6. 了解木马的分类与发展
素质目标	1. 掌握网络安全行业的基本情况 2. 具有良好的团队协作和沟通交流能力 3. 培养良好的职业道德 4. 树立较强的安全、节约、环保意识

5.4　任务实施

5.4.1　任务1：使用pcAnywhere远程控制计算机

1. 任务目标

了解pcAnywhere远程控制的工作原理，熟练掌握pcAnywhere被控端和主控端的配置方法，实现在本地计算机上控制远程计算机，使得两地的计算机可以协同工作。

2. 工作任务

(1) 被控端的配置；

(2) 主控端的配置；

(3) 远程控制的实现。

3. 工作环境

(1) 两台预装Windows Server 2003/XP的主机，通过网络相连。

(2) 软件工具：pcAnywhere软件。

4. 实施过程

(1) 被控端的配置

① 打开pcAnywhere主窗口，然后单击"pcAnywhere管理器"子窗口下的"被控端"按钮，再单击"动作"子窗口下的"添加"按钮，在出现的"联机向导-联机方式"对话框中，单击"下一步"按钮，如图5-1所示。

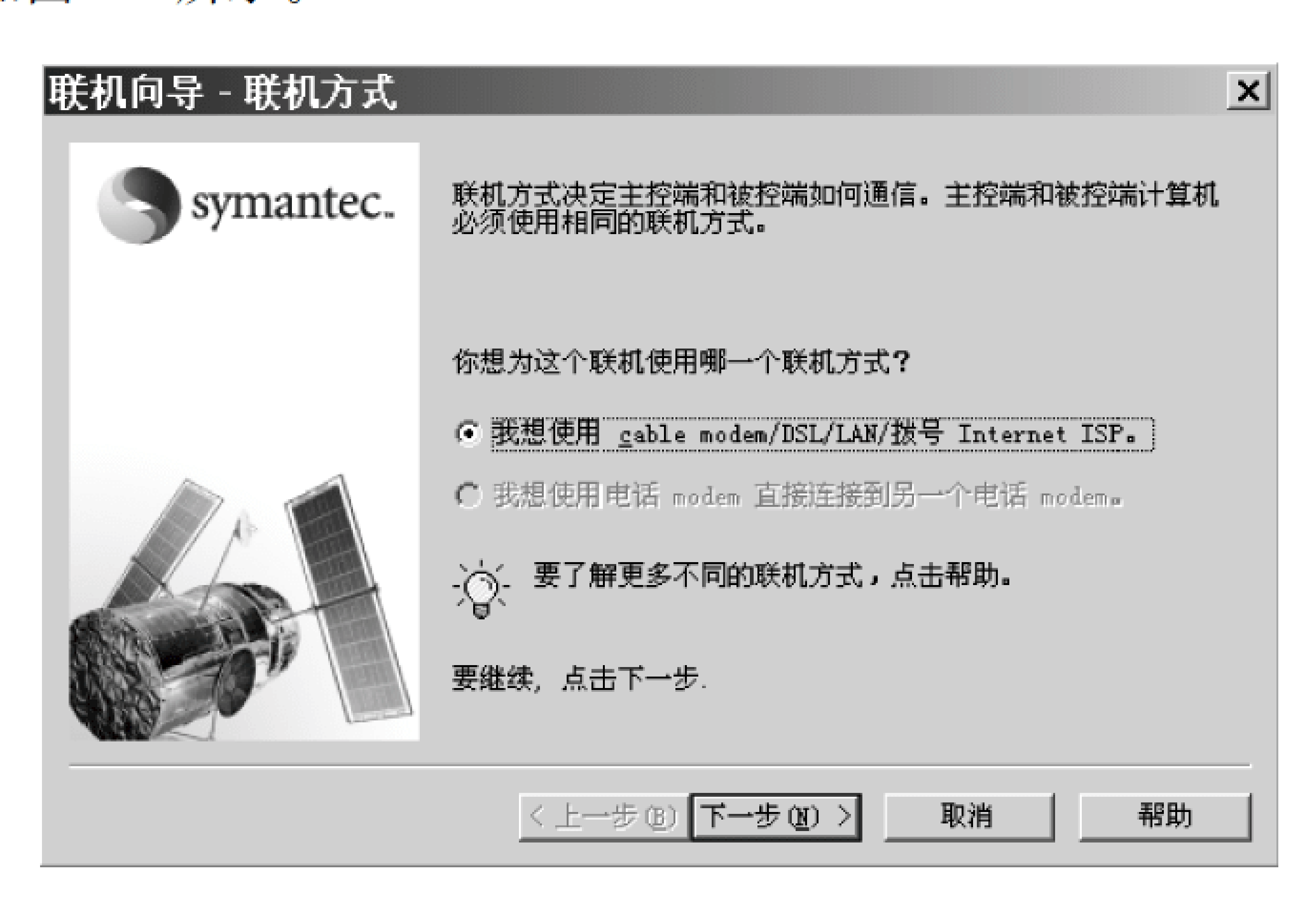


图5-1　"联机向导-联机方式"对话框(1)

② 在弹出的"联机向导-验证类型"中，勾选"我想建立一个用户名和密码"，然后单击"下一步"按钮，如图5-2所示。

③ 在弹出的"联机向导-用户名和密码"对话框中输入登录被控端时的用户名和密码，然后单击"下一步"按钮，如图5-3所示。

④ 在弹出的"联机向导-摘要"对话框中，勾选"联机向导结束后等待主控端计算机联机"，并单击"完成"按钮，如图5-4所示。



图 5-2 “联机向导-验证类型”对话框



图 5-3 “联机向导-用户名和密码”对话框

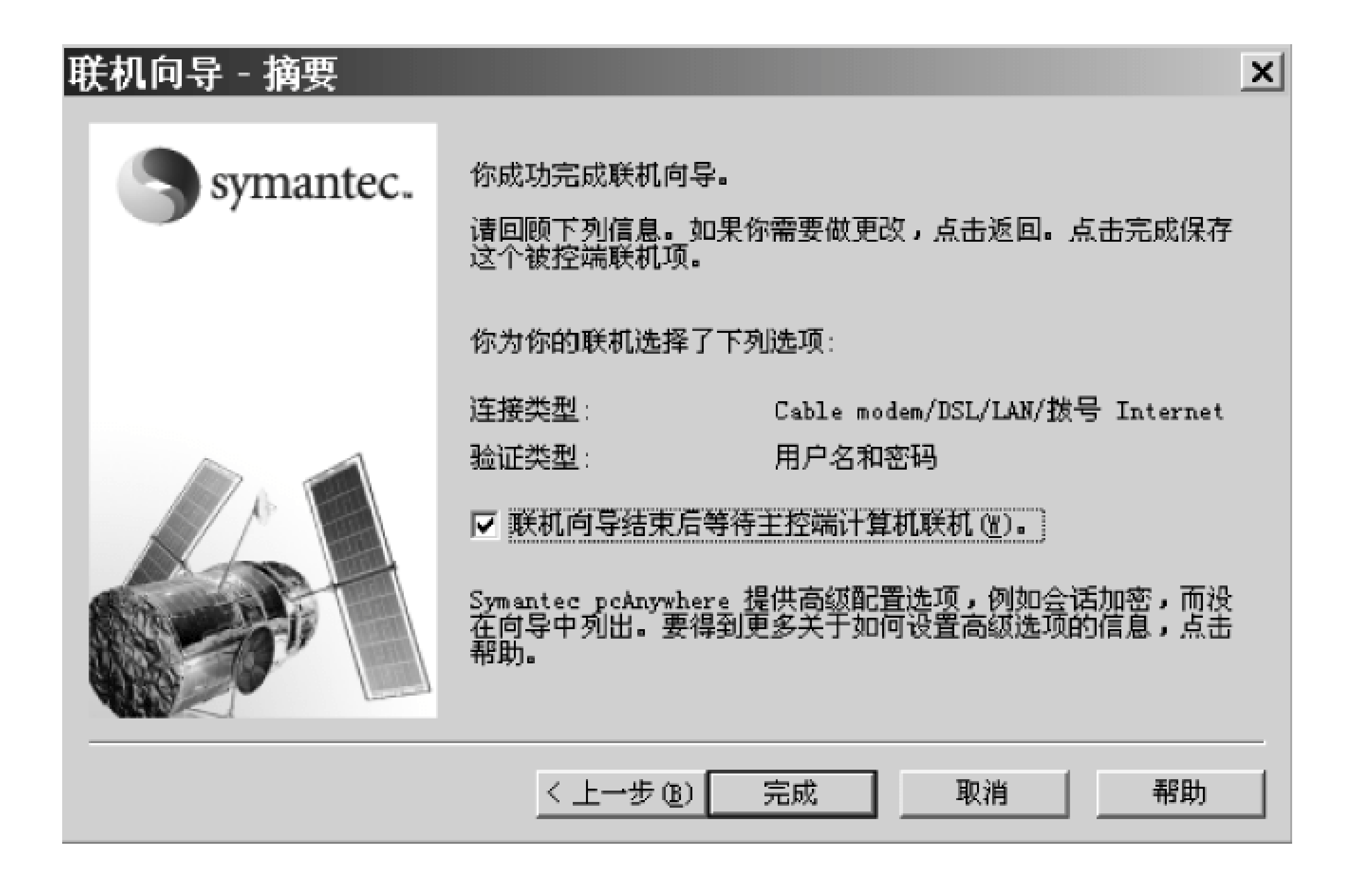


图 5-4 “联机向导-摘要”对话框(1)

⑤ 完成后需对被控端进行设置。选中 pcAnywhere 主窗口中“被控端”子窗口中的“新被控端”图标，然后单击“动作”子窗口中的“属性”按钮，如图 5-5 所示。

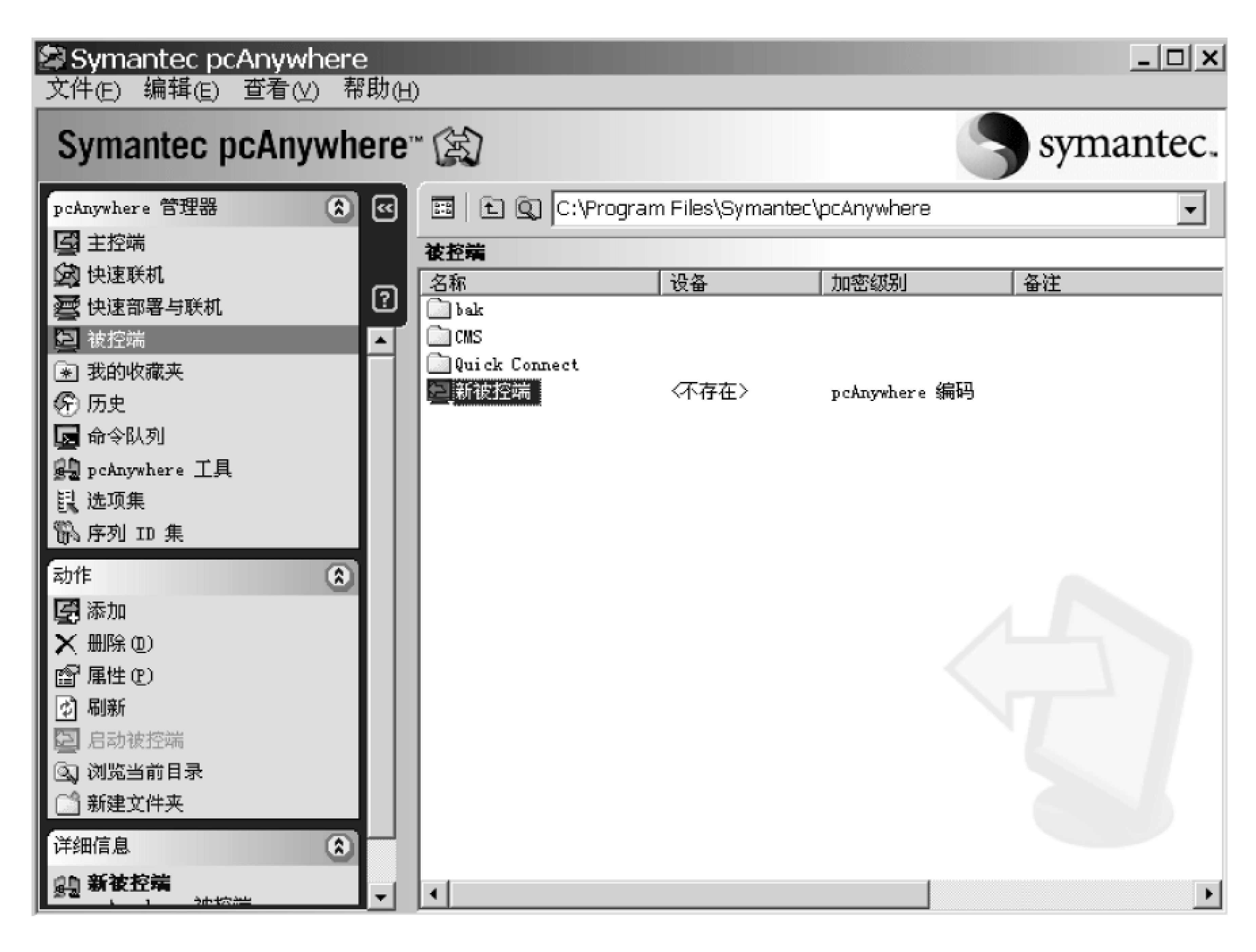


图 5-5　pcAnywhere 主窗口(1)

⑥ 在弹出的“被控端 属性：新被控端”对话框中选择“连接信息”选项卡，在设备列表中选中“TCP/IP”选项。如果是局域网，也可以选用 SPX、NetBIOS 协议，然后单击“应用”按钮，如图 5-6 所示。

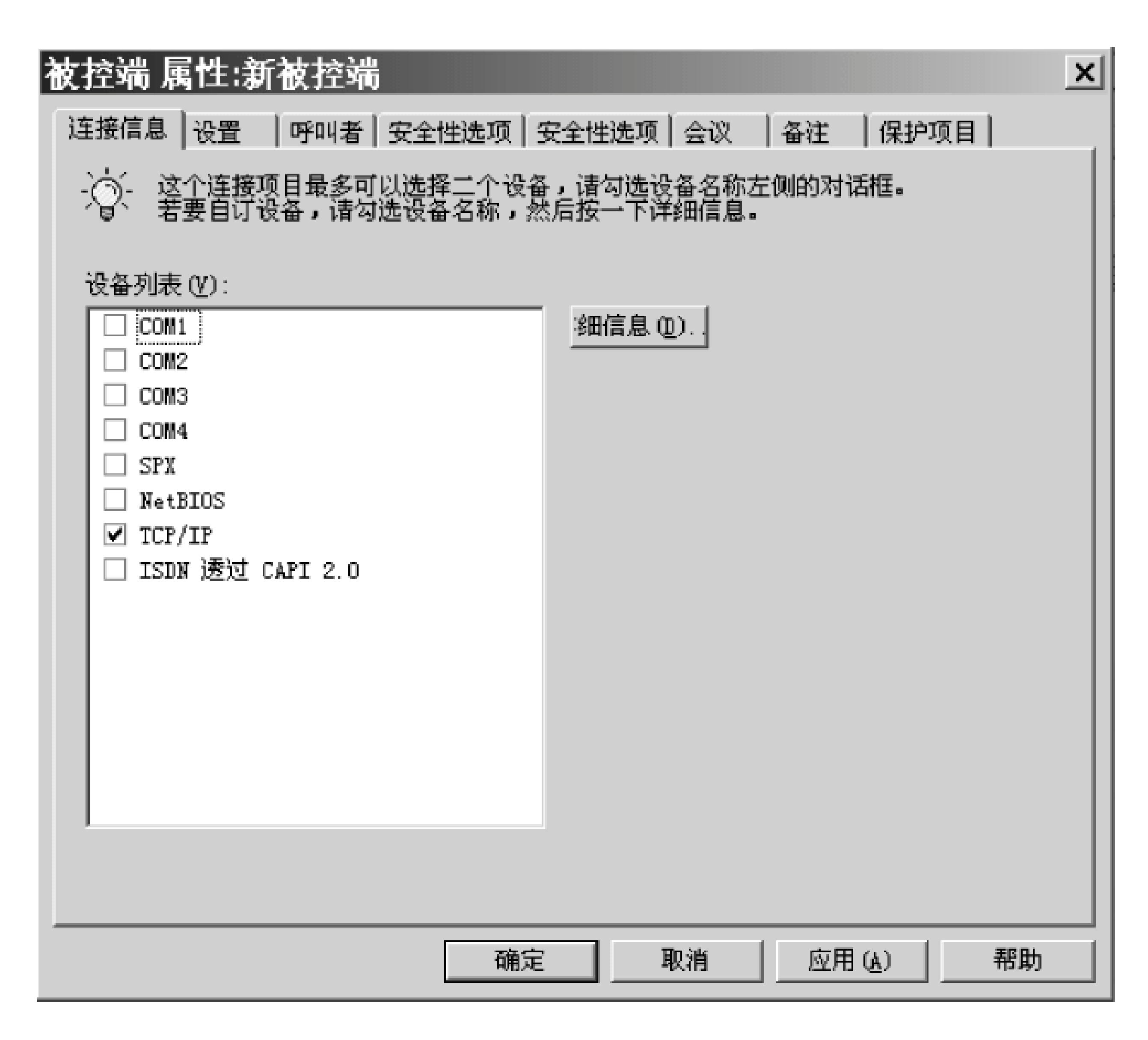


图 5-6　“被控端 属性：新被控端”对话框

⑦ 选择“呼叫者”选项卡，然后右击呼叫者“属性”按钮。

⑧ 选择“权限”选项卡，将“呼叫者权限”设置为超级用户，并依次单击“应用”和“确定”按钮，如图 5-7 所示。



图 5-7 “权限”选项卡

(2) 主控端的配置

① 打开 pcAnywhere 主窗口，然后单击“pcAnywhere 管理器”子窗口下的“主控端”按钮，再单击“动作”子窗口下的“添加”按钮。在出现的“联机向导-联机方式”对话框中，单击“下一步”按钮，如图 5-8 所示。



图 5-8 “联机向导-联机方式”对话框(2)

② 在出现的“联机向导-目标地址”对话框中输入被控端计算机的 IP 地址，然后单击“下一步”按钮，如图 5-9 所示。如果在局域网中，也可以不加设置，主控端会从网络中搜索所有开启的被控端计算机。

③ 如果想让主控端在联机向导结束后联机到被控端，可在弹出的“联机向导-摘要”对话框中勾选“联机向导结束后，联机到一个被控端”选项，然后单击“完成”按钮，如图 5-10 所示。

④ 设置主控端的属性。选中 pcAnywhere 主窗口中“主控端”子窗口中的“新的主控端”图标，然后单击“动作”子窗口中的“属性”按钮，如图 5-11 所示。

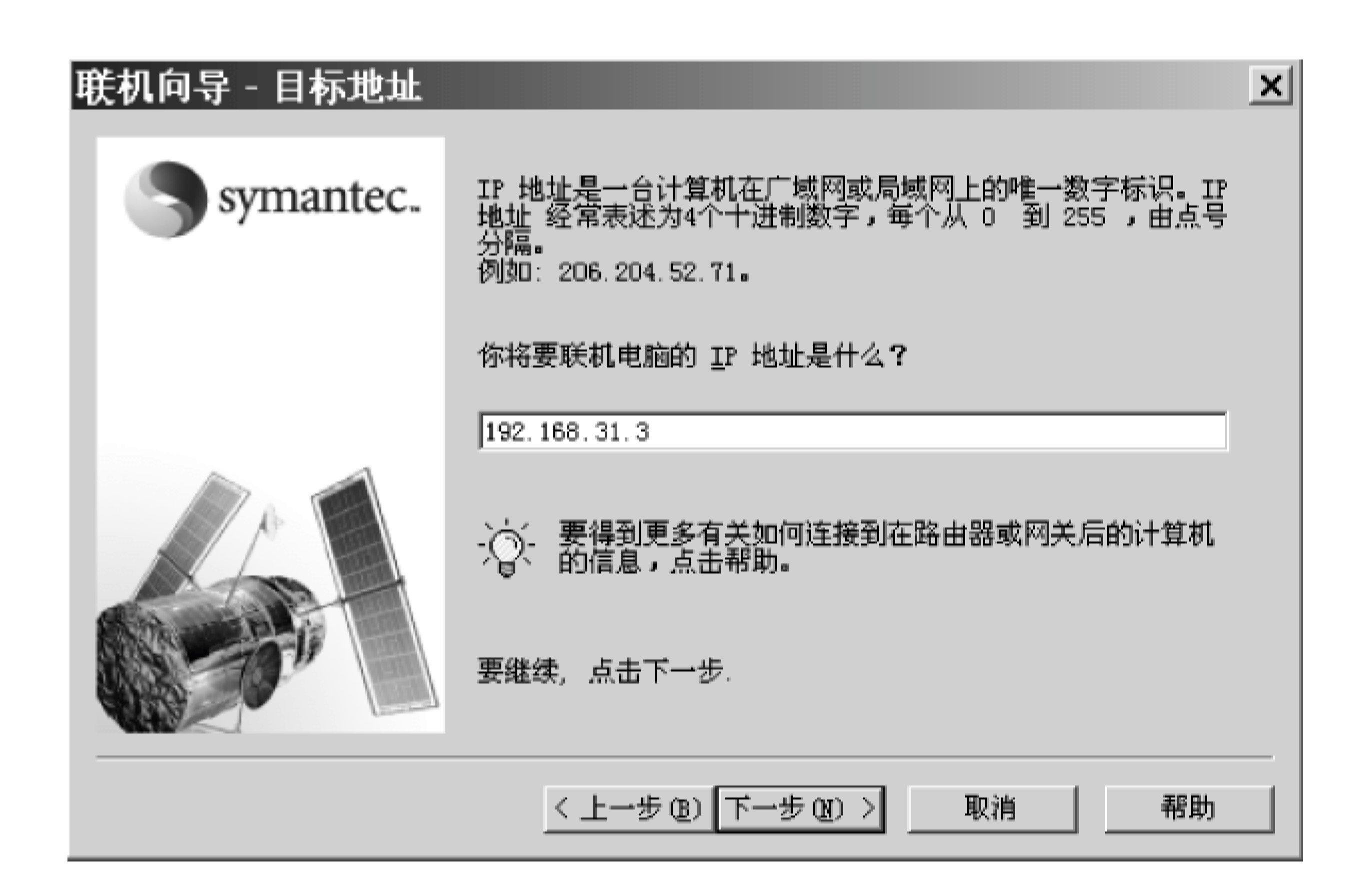


图 5-9 “联机向导-目标地址”对话框



图 5-10 “联机向导-摘要”对话框(2)

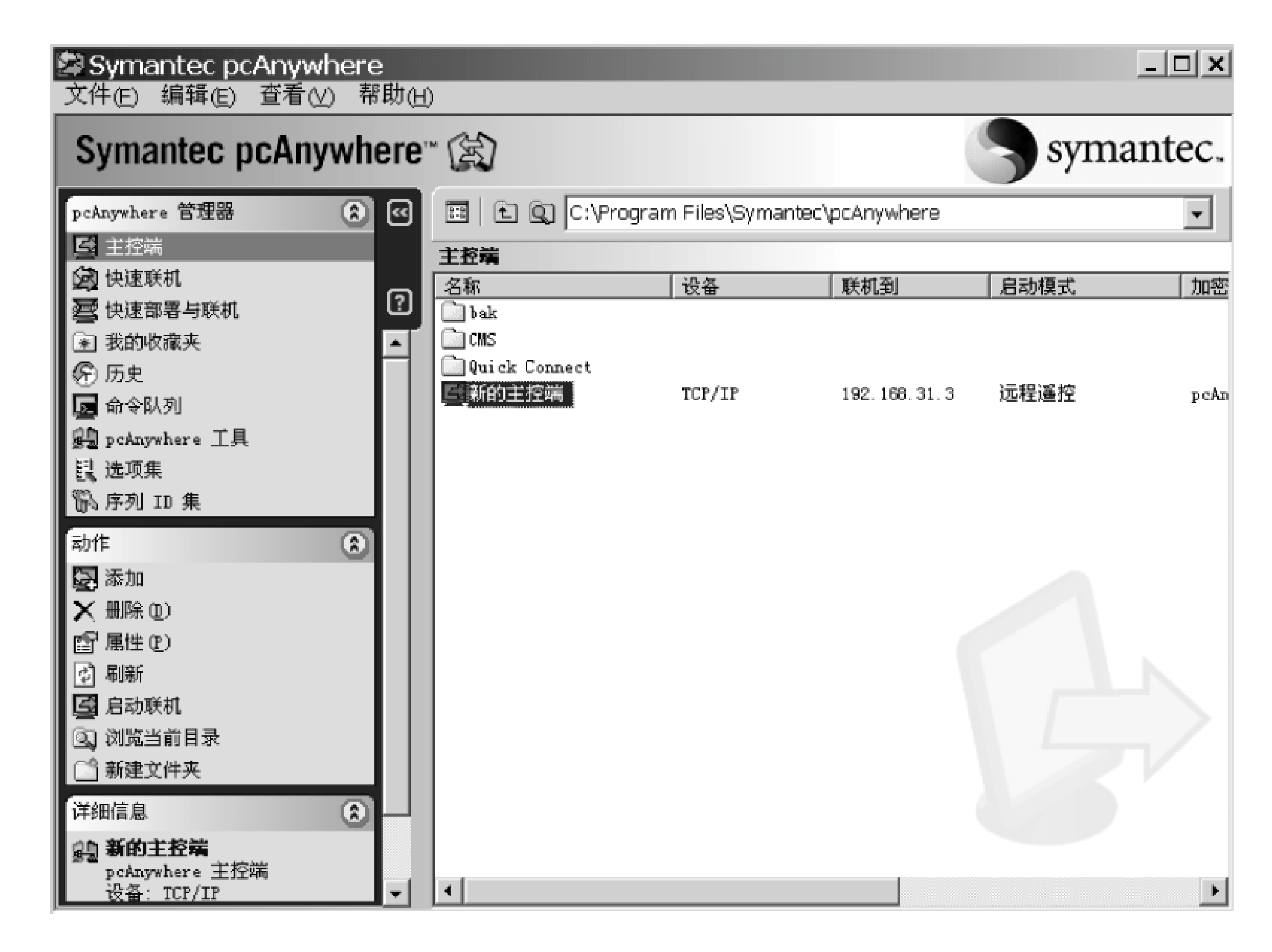


图 5-11 pcAnywhere 主窗口(2)

⑤ 在弹出的"主控端 属性：新的主控端"对话框中选择"连接信息"选项卡，在设备列表中选中"TCP/IP"选项。如果是局域网，也可以选用 SPX、NetBIOS 协议，并单击"应用"按钮，如图 5-12 所示。

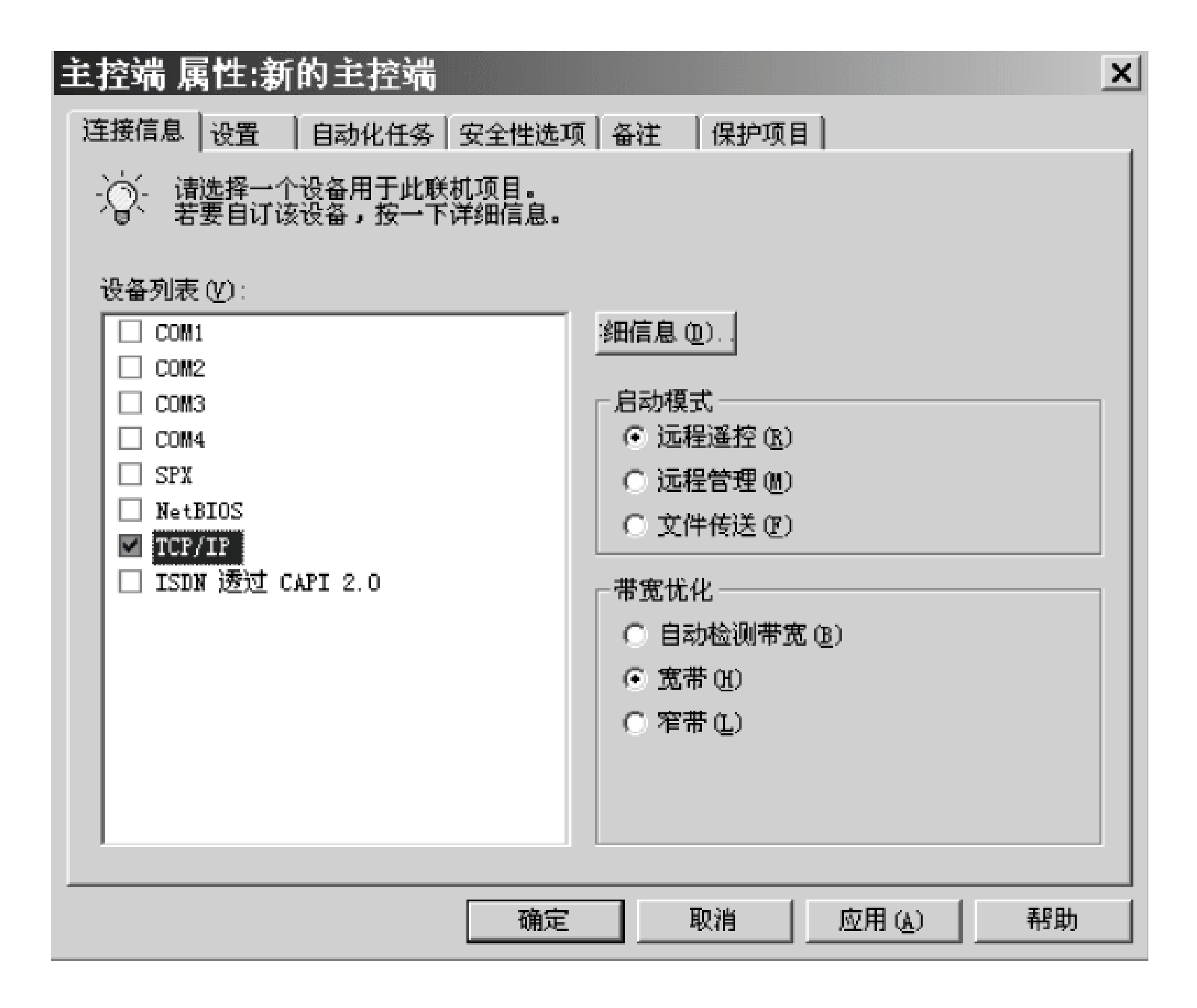


图 5-12 "主控端 属性：新的主控端"对话框

⑥ 在"设置"选项卡中，确认要控制的网络被控端 PC 或 IP 地址，并在登录信息栏勾选"一旦连接即自动登入至被控端"。在登录名称和密码处输入被控端的登录名与密码，并依次单击"应用"和"确认"按钮。

(3) 远程控制的实现

① 在被控端主机的 pcAnywhere 主窗口双击新建的被控端图标，使其处于等待状态。

② 在主控端的 pcAnywhere 主窗口双击新建的主控端图标，即可开始远程连接。

③ 在主控端与被控端连接成功后，被控端的桌面将出现在主控端的主窗口中。用鼠标单击窗口的桌面，就可以像使用本地计算机一样操作远程计算机了。通过窗口上部的按钮，还可以进行文件传输、语音对话、屏幕捕获、重启被控端等操作。

④ 如果要停止远程控制的操作，可单击窗口上方的"结束会话"按钮。

5.4.2 任务 2：使用 QuickIP 对多点计算机进行远程控制

1. 任务目标

熟练掌握使用 QuickIP 通过局域网或互联网全权控制远程计算机。服务器可以同时被多台客户机控制，一台客户机也可以同时控制多台服务器。利用 QuickIP，以树状展示远程计算机所有磁盘驱动器的内容，对远程屏幕进行录像，控制远程主机的鼠标、键盘，控制远程计算机的所有进程、窗口、程序，控制远程主机重新启动、关机、登录等。

2. 工作任务

(1) 设置 QuickIP 服务器密码；

(2) 登录客户端；

(3) 查看 QuickIP 服务器信息。

3. 工作环境

（1）两台预装 Windows Server 2003/XP 的主机，通过网络相连。

（2）软件工具：QuickIP 软件。

4. 实施过程

（1）设置 QuickIP 服务器密码

QuickIP 具有安全的密码验证功能，客户端必须知道服务器端的密码才能进行控制。因此，在第一次启动 QuickIP 服务器程序时，会提示设置本地服务器的密码，具体的操作步骤如下：

① 启动 QuickIP 服务器时会弹出一个提示对话框，提示用户设置密码，单击“确定”按钮即可，如图 5-13 所示。

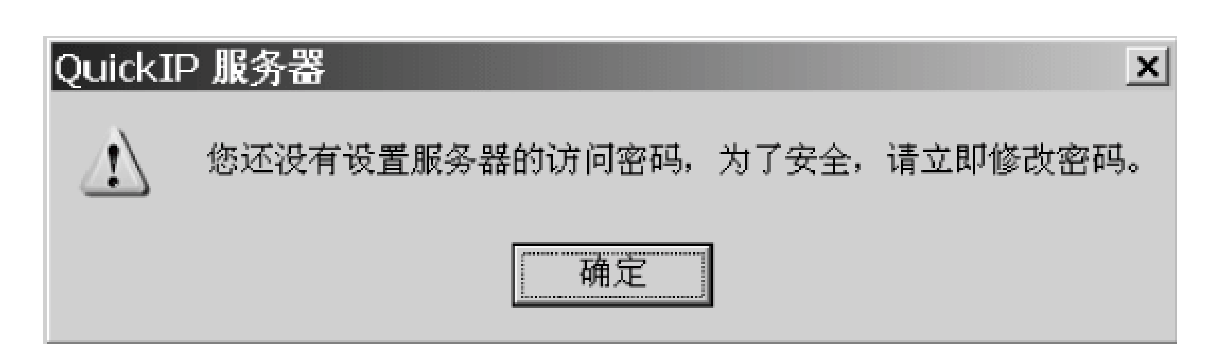


图 5-13　设置密码提示窗

② 在“修改本地服务器的密码”对话框中输入要设置的密码，然后单击“确认”按钮，如图 5-14 所示。

③ 密码修改成功后会弹出一个提示对话框，单击“确定”按钮关闭，如图 5-15 所示。

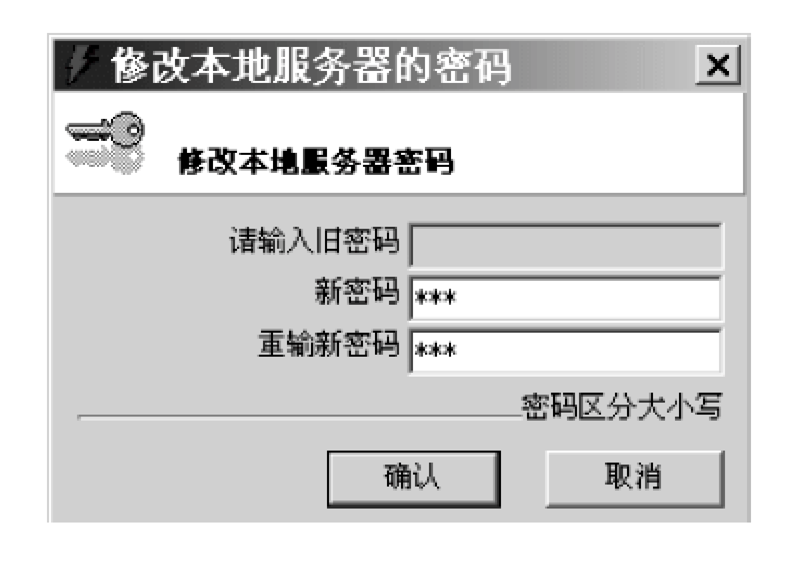




图 5-14　“修改本地服务器的密码”对话框(1)



图 5-15　密码修改成功提示窗

（2）登录客户端

① 启动黄色图标的“QuickIP 客户机”程序，然后在工具栏中单击“添加主机”按钮，如图 5-16 所示。



图 5-16　“QuickIP 客户机”主窗口

② 输入要添加主机的 IP 地址、端口以及密码，然后单击“确认”按钮，如图 5-17 所示。

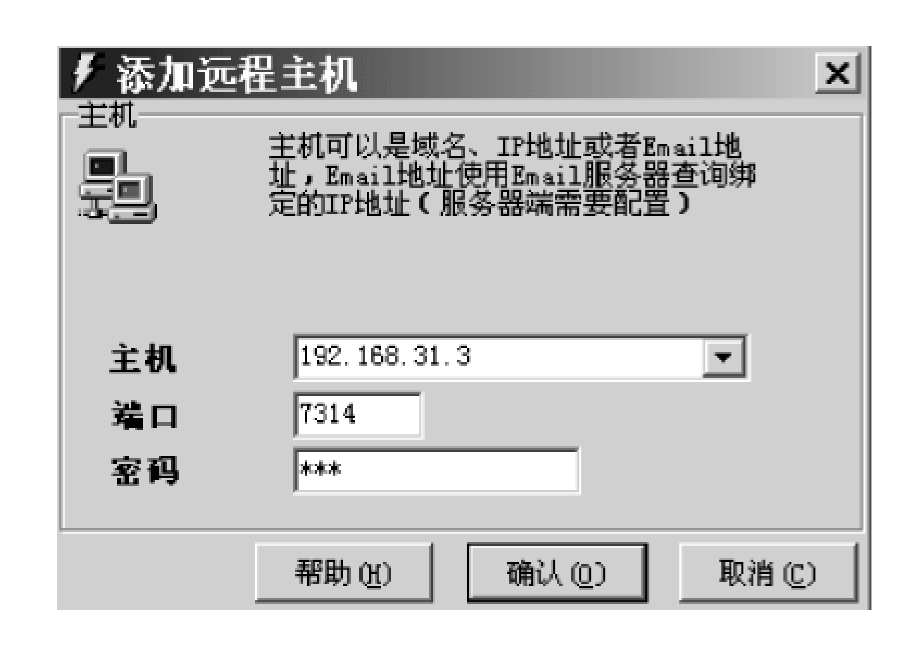


图 5-17 “添加远程主机”对话框

③ 返回客户端主窗口，单击刚添加的远程主机 IP 地址前面的“＋”号，即可看到所有的远程控制功能，如图 5-18 所示。

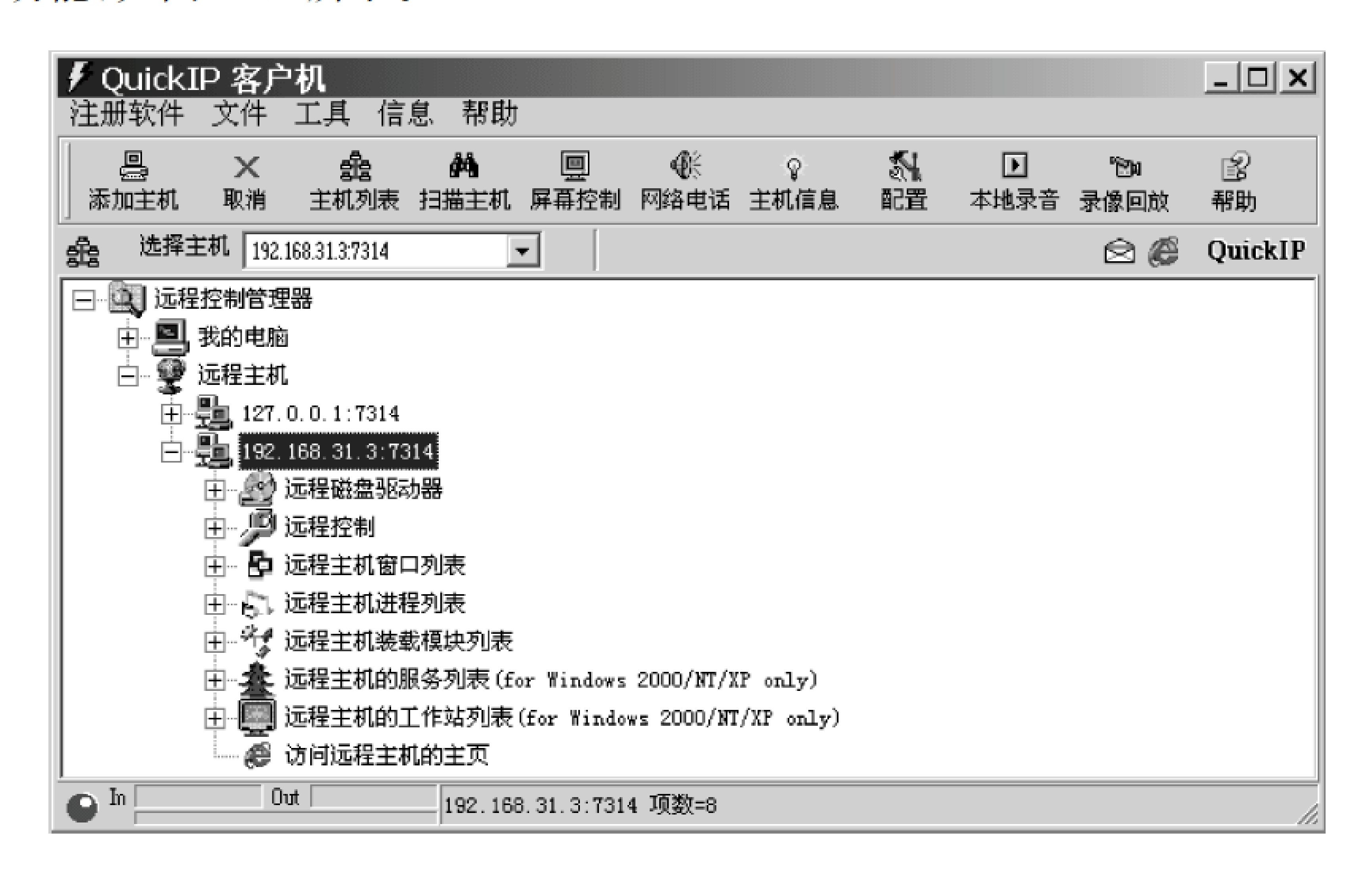


图 5-18 客户端主窗口

④ 单击“远程磁盘驱动器”选项，弹出登录对话框，输入登录密码后单击“确认”按钮完成登录，如图 5-19 所示。



图 5-19 登录提示框

⑤ 登录成功后，可以看到远程目标主机的所有磁盘驱动器盘符。可以对磁盘进行任何操作，如图 5-20 所示。

⑥ 展开“远程控制”项，然后双击“屏幕控制”，即可实现远程屏幕控制操作，如图 5-21 所示。

⑦ 在“QuickIP 客户机”的工具栏中单击“主机列表”按钮，如图 5-22 所示。

⑧ 在“编辑远程主机”对话框中可添加、删除、修改远程主机。设置完成后单击“保存”按钮退出，如图 5-23 所示。



图 5-20　磁盘操作菜单

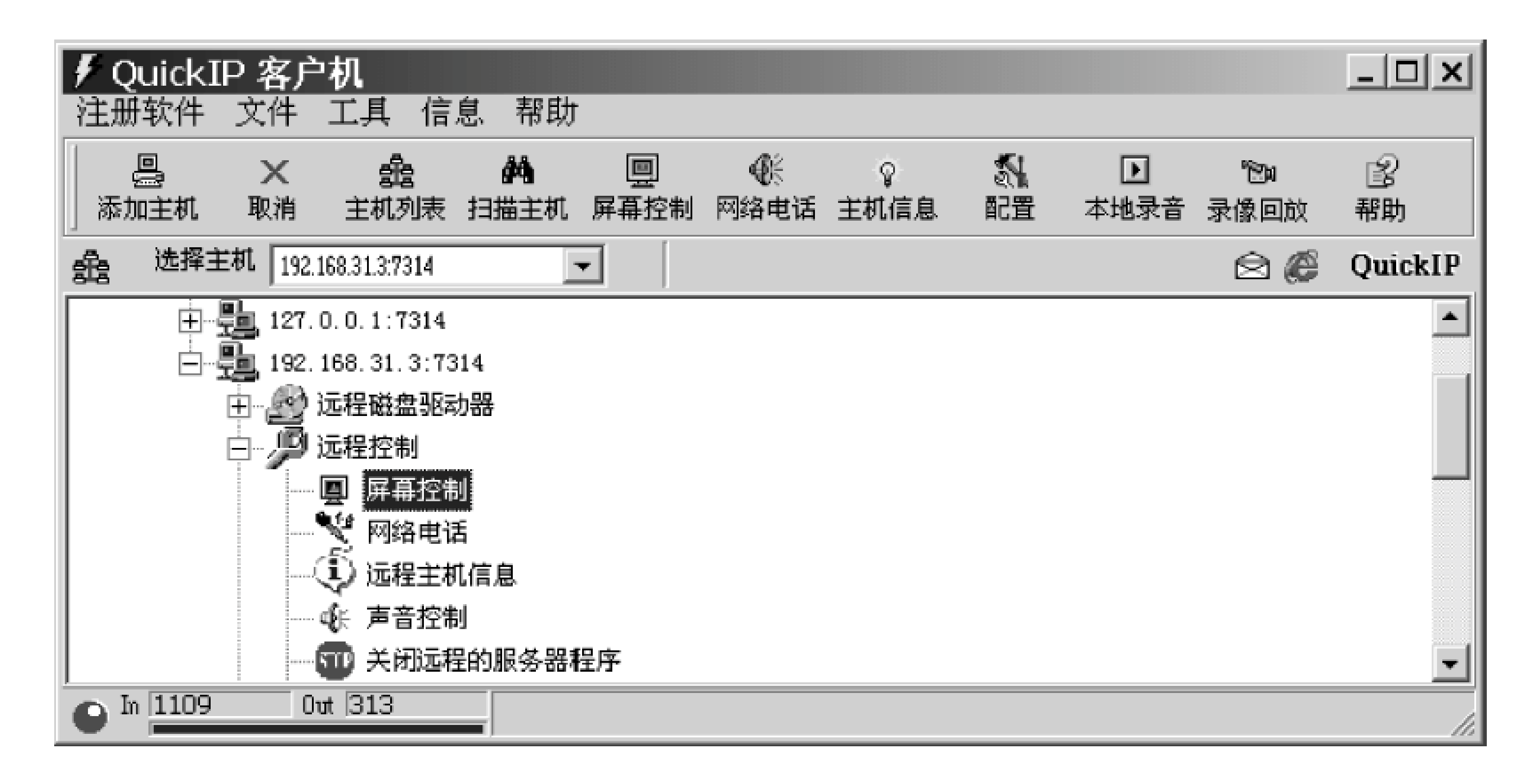


图 5-21　“远程控制”项



图 5-22　“主机列表”按钮　　　　图 5-23　“编辑远程主机”对话框

(3) 查看 QuickIP 服务器信息

① 启动红色图标的“QuickIP 服务器管理”程序，在其主界面中可以看到客户机上的所有操作信息，如图 5-24 所示。

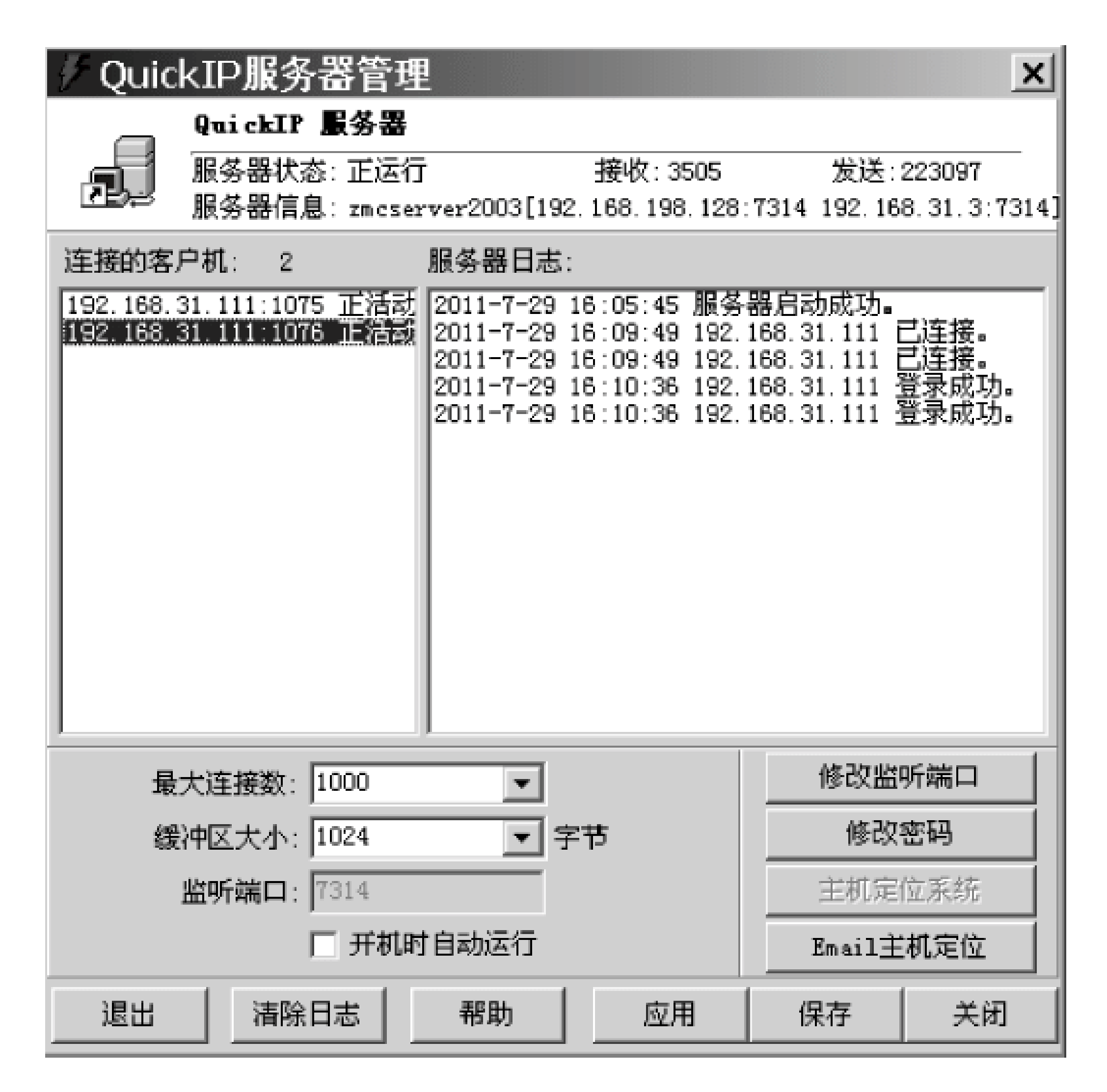


图 5-24 “QuickIP 服务器管理”主窗口

② 在“QuickIP 服务器管理”对话框中单击“修改监听端口”按钮，如图 5-25 所示。

③ 在“修改服务器监听端口”对话框中清除“使用默认的监听端口”复选框即可修改端口。修改后，单击“确认”按钮。

④ 在“QuickIP 服务器管理”对话框中单击“修改密码”按钮，打开“修改本地服务器的密码”对话框。

⑤ 在“修改本地服务器的密码”对话框的第一个文本框中输入以前的密码，在后面的两个文本框中输入相同的修改后的密码，然后单击“确认”按钮，如图 5-26 所示。

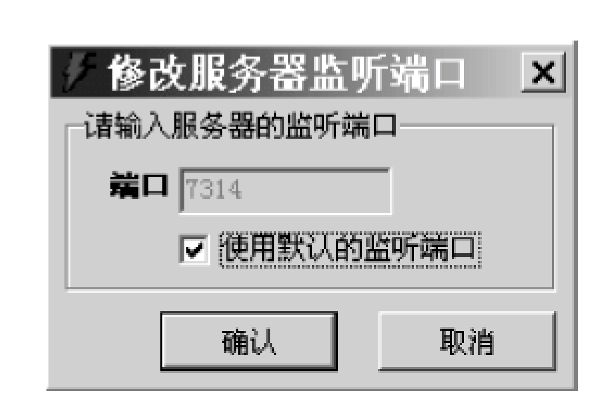


图 5-25 “修改服务器监听端口”对话框

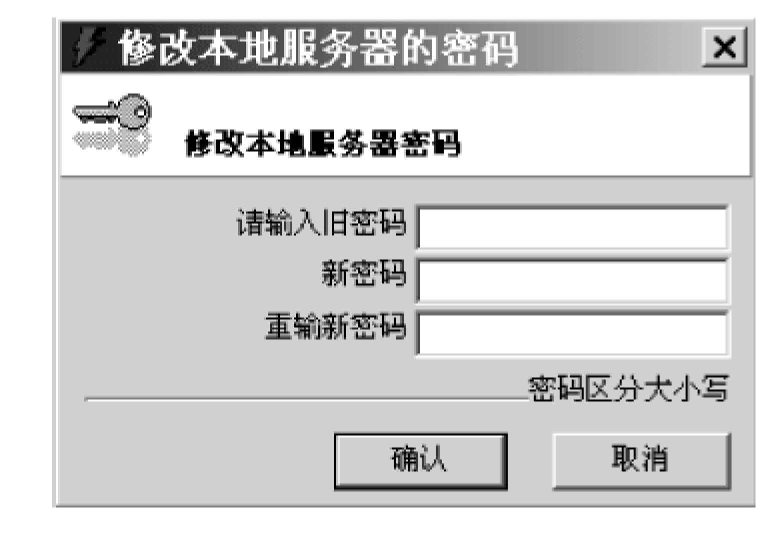


图 5-26 “修改本地服务器的密码”对话框(2)

5.4.3 任务 3：使用“任我行”软件对远程计算机进行控制

1. 任务目标

熟练掌握“任我行”软件服务端的配置方法，能利用该软件对目标计算机进行捕获屏幕、视频监控、服务管理、进程管理、注册表监控等操作。

2. 工作任务

(1) 配置正向连接型服务端；

(2) 配置反向连接型服务端；

(3) 通过服务端程序进行远程控制。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机,通过网络相连。

(2) 软件工具:“任我行”软件。

4. 实施过程

“任我行”软件与“灰鸽子”软件的设置和使用非常相似,都需要生成服务端。只有通过这种生成的服务端,木马程序才能被黑客远程控制。具体的操作步骤如下:

(1) 配置正向连接型服务端

① 打开“任我行”软件的主窗口,然后单击“配置服务端”按钮,如图 5-27 所示。



图 5-27　“任我行”软件主窗口

② 在打开的“选择配置类型”对话框中列出了 5 种配置情况,用户可根据情况选择合适的方式。这里介绍配置正向连接型服务端的方法,因此单击“正向连接型”按钮,如图 5-28 所示。

③ 在打开的“正向连接”对话框中,如果用户想修改服务端的显示图标,可在“服务端图标修改”框中单击“更换图标”按钮,如图 5-29 所示。



图 5-28　“选择配置类型”对话框(1)

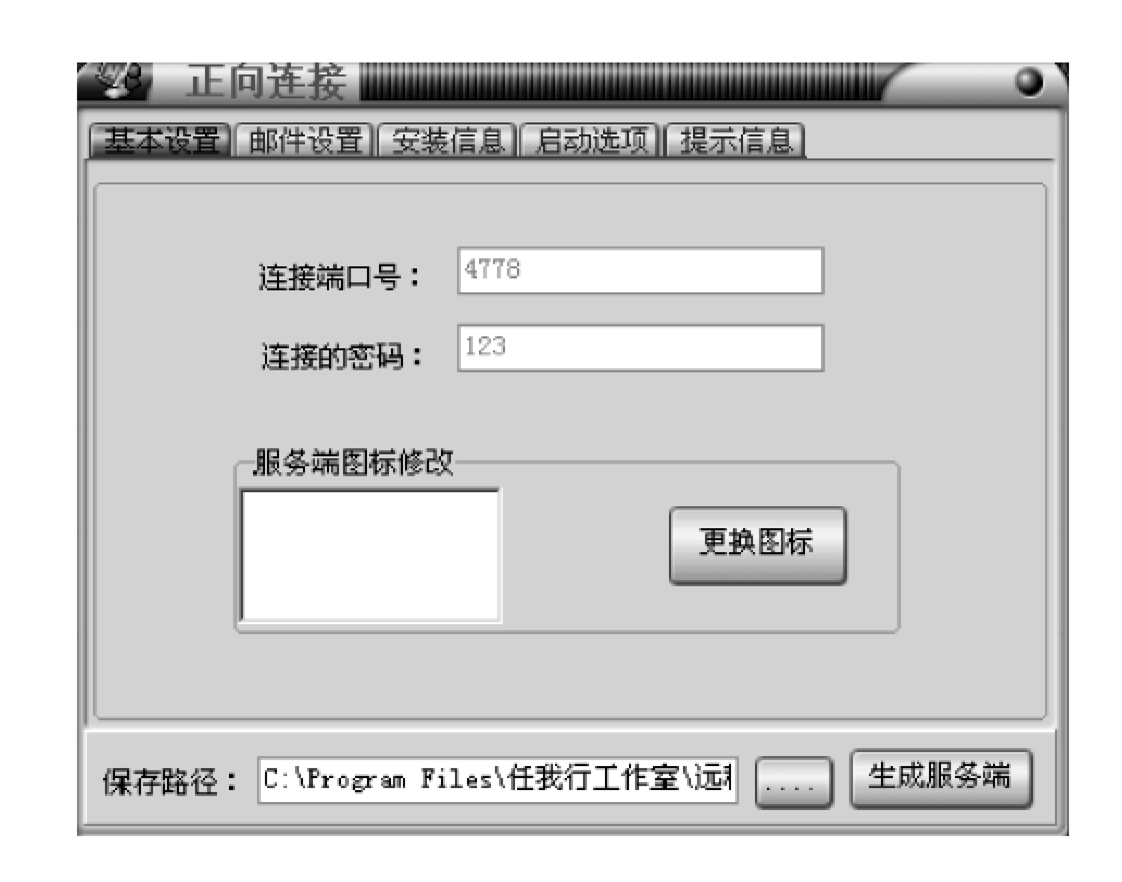


图 5-29　“正向连接”对话框

④ 在打开的“打开”对话框中选择需要的图标样式,然后单击“打开”按钮返回“正向连接”对话框,如图 5-30 所示。



图 5-30 “打开”对话框

⑤ 切换到“邮件设置”选项卡，在该选项界面中可以设置使用邮箱接收 IP 信息，一般情况下，这里的选项保持默认设置即可，如图 5-31 所示。

⑥ 切换到“安装信息”选项卡，在此可以改变服务端安装路径和服务端安装名称等信息。一般情况下，黑客在配置服务端时会选择“自动隐藏安装文件”复选框和“2000/XP/2003 系统中隐藏进程”复选框，以增强服务端的隐蔽性，不容易被发现，如图 5-32 所示。

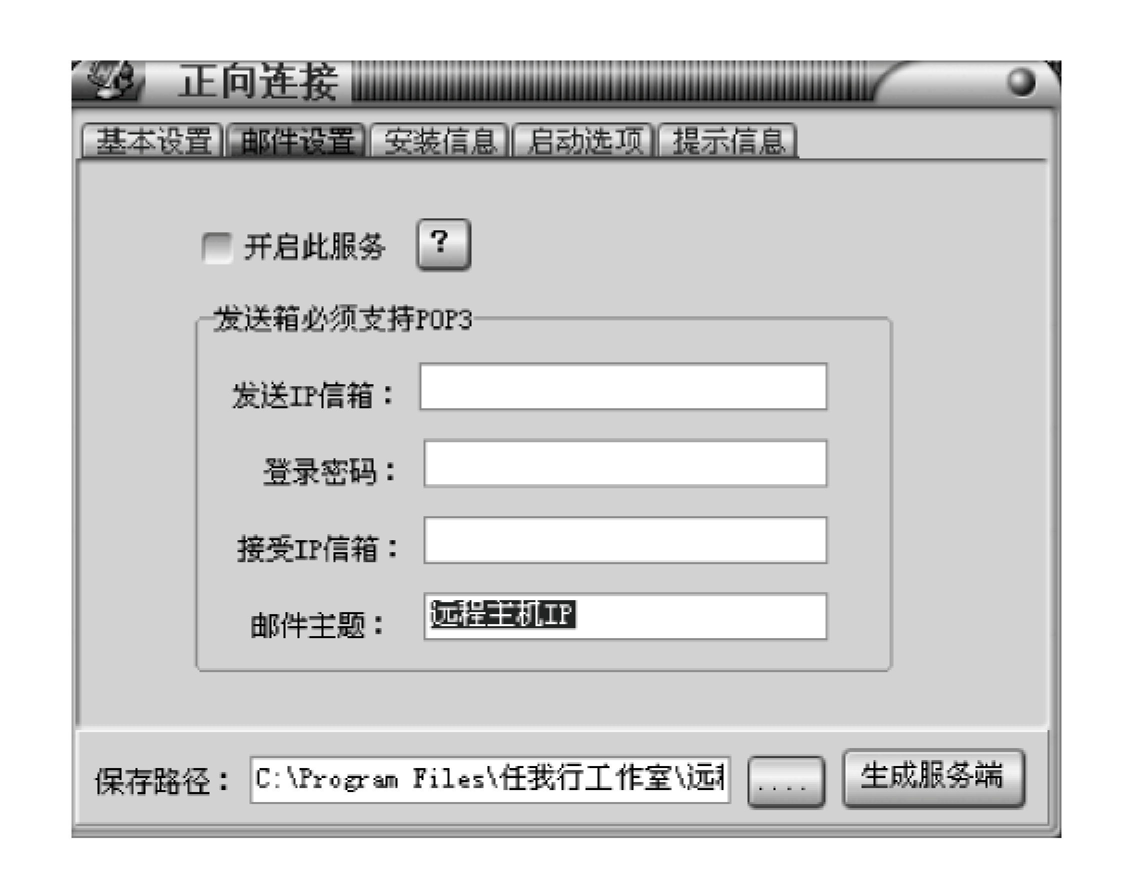


图 5-31 “邮件设置”选项卡

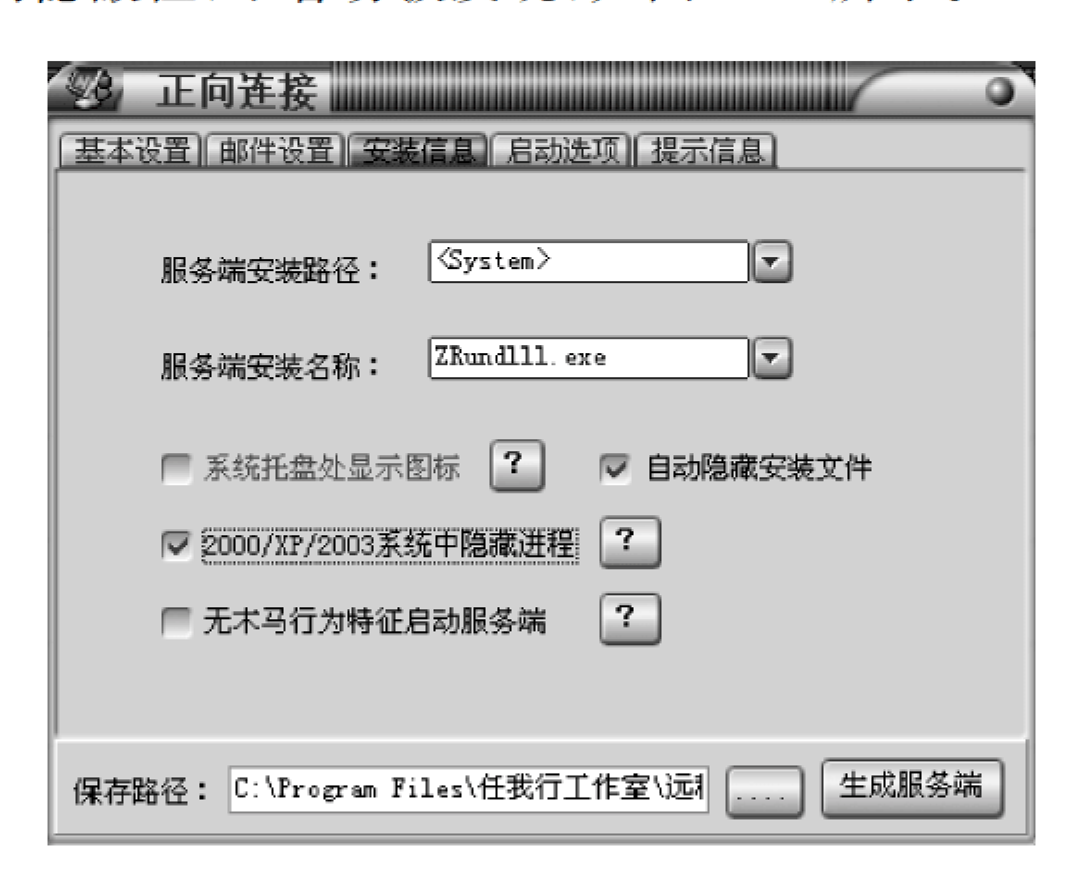


图 5-32 “安装信息”选项卡(1)

⑦ 设置完成后切换到“启动选项”选项卡，然后选中“远程主机是 Win9X 写入注册表启动项”和“远程主机是 2000/XP 注册为服务启动”复选框。在“服务启动项”组合框中，黑客通常会更改显示名称、服务名称及描述信息，以便增强服务端的隐蔽性。在此保持默认设置，如图 5-33 所示。

⑧ 切换到“提示信息”选项卡，然后选中“安装完成后显示的提示信息”复选框，并在“信息标题”、“信息正文”文本框及“图标类型”、“按钮类型”下拉列表文本框中设置提示信息，如图 5-34 所示。

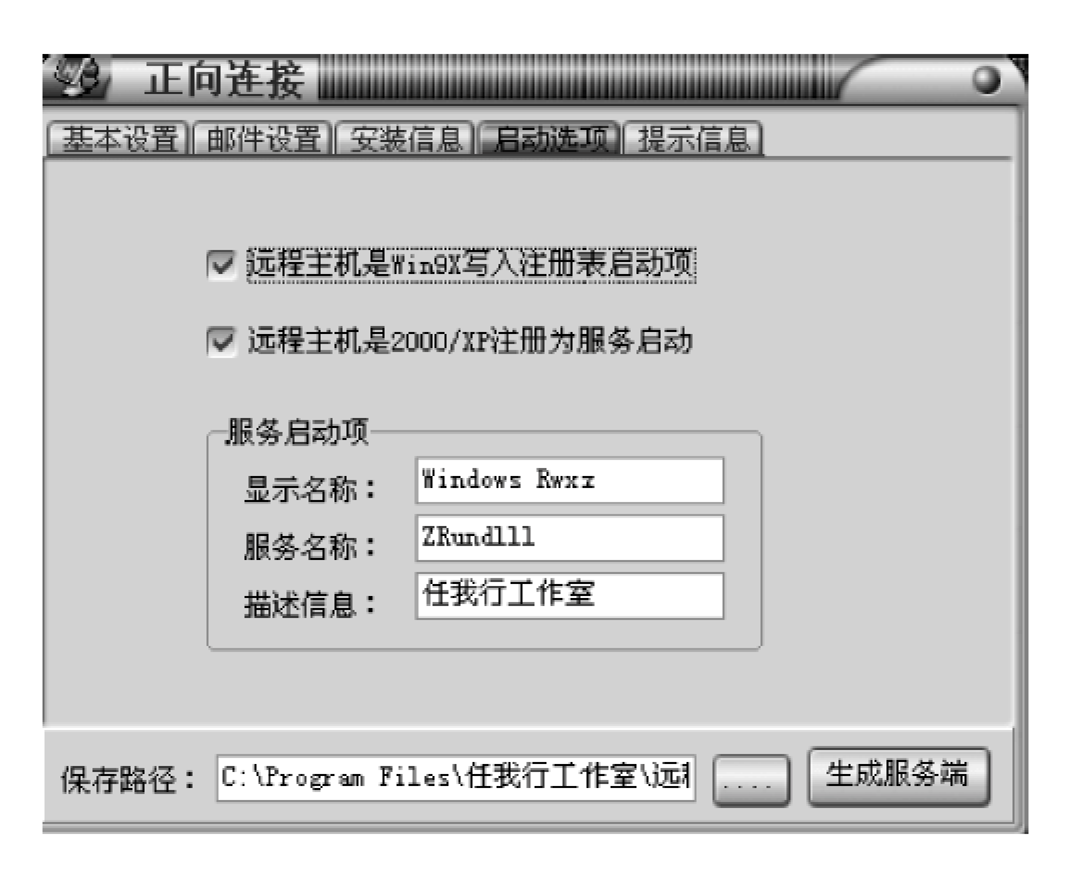


图 5-33　“启动选项”选项卡

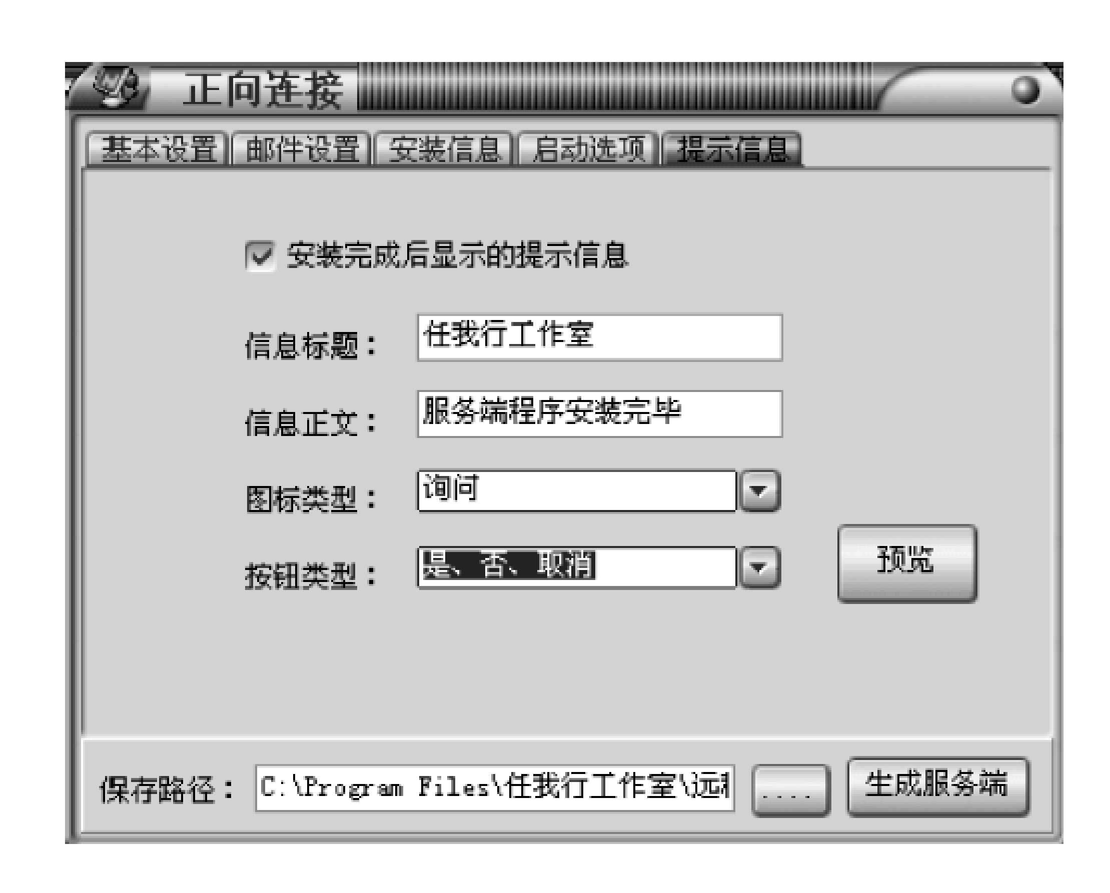


图 5-34　“提示信息”选项卡(1)

⑨ 生成服务端后，如果用户中了木马程序，通常会显示设置的提示信息。提示信息设置完成后，单击“预览”按钮进行预览，如图 5-35 所示。

⑩ 为了增强服务端程序的隐蔽性，黑客通常会撤选“安装完成后显示的提示信息”复选框。这里同样不选中该复选框，如图 5-36 所示。接下来，需要设置服务端程序的保存路径。

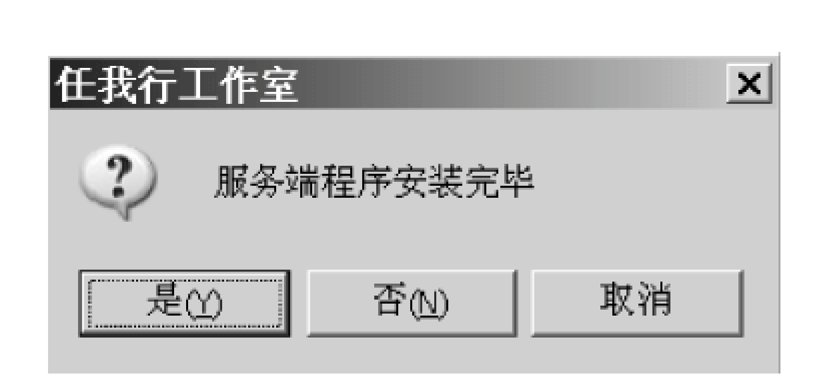


图 5-35　预览效果

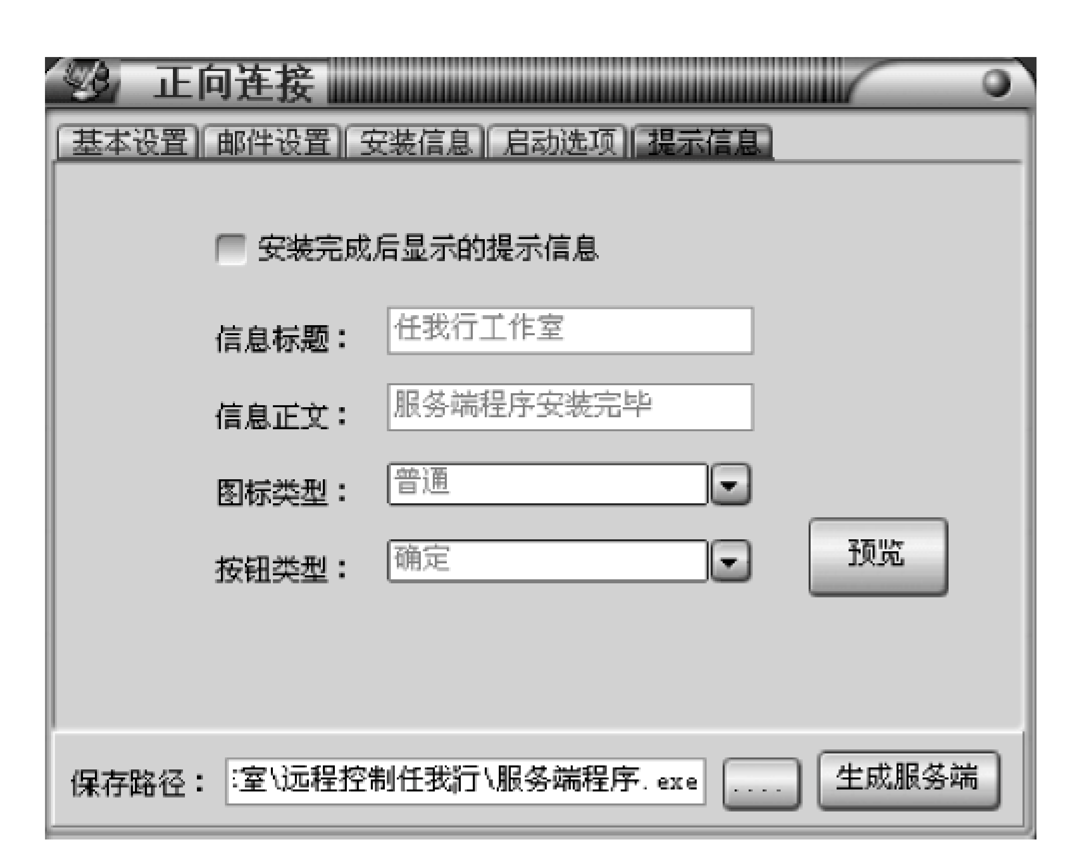


图 5-36　“提示信息”选项卡(2)

⑪ 在“正向连接”对话框底部的“保存路径”文本框中设置服务程序的保存路径，然后单击“生成服务端”按钮，服务端程序生成之后会打开一个提示对话框，如图 5-37 所示。

⑫ 单击提示对话框中的“确定”按钮，此时正向连接型服务端程序就成功生成了，如图 5-38 所示。

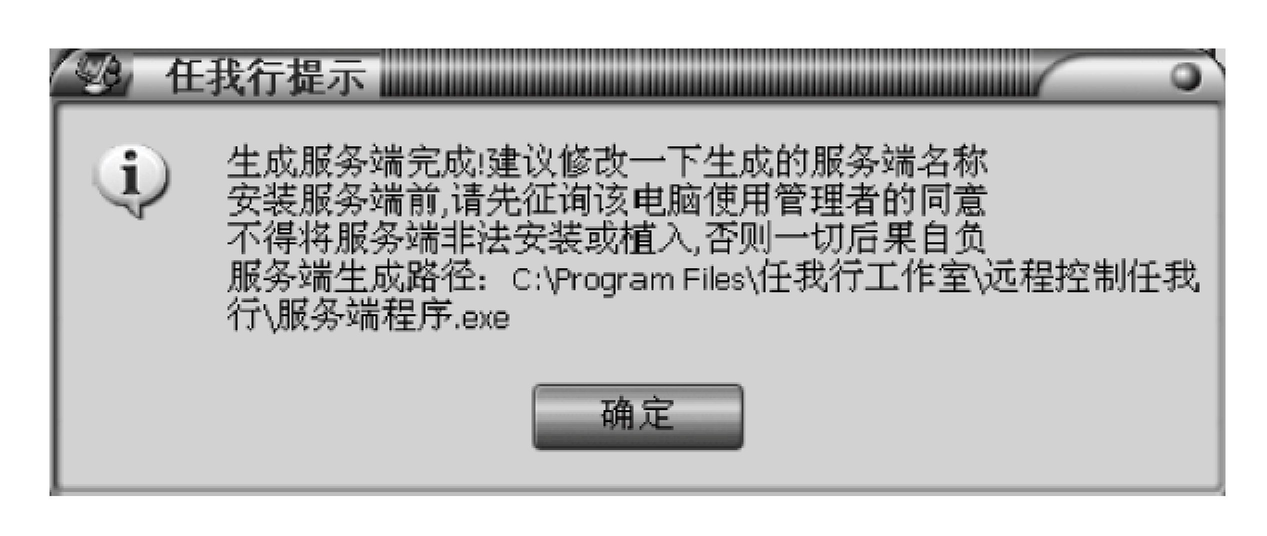


图 5-37　“任我行提示”窗口



图 5-38　正向连接型服务端程序

（2）配置反向连接型服务端

① 在“任我行”程序的主窗口中单击“配置服务端”按钮，打开“选择配置类型”对话框，如图 5-39 所示。

② 单击对话框中的“反向连接型”按钮，打开“反向连接”对话框。切换到“自动上线”选项卡，然后在“DNS 解析域名”下拉列表文本框中选择本机的域名解析地址。在“连接密码”文本框中可以设置一个连接密码，还可以更改主机上图像的显示样式及服务端的图标，如图 5-40 所示。设置完成后，切换到“安装信息”选项卡。

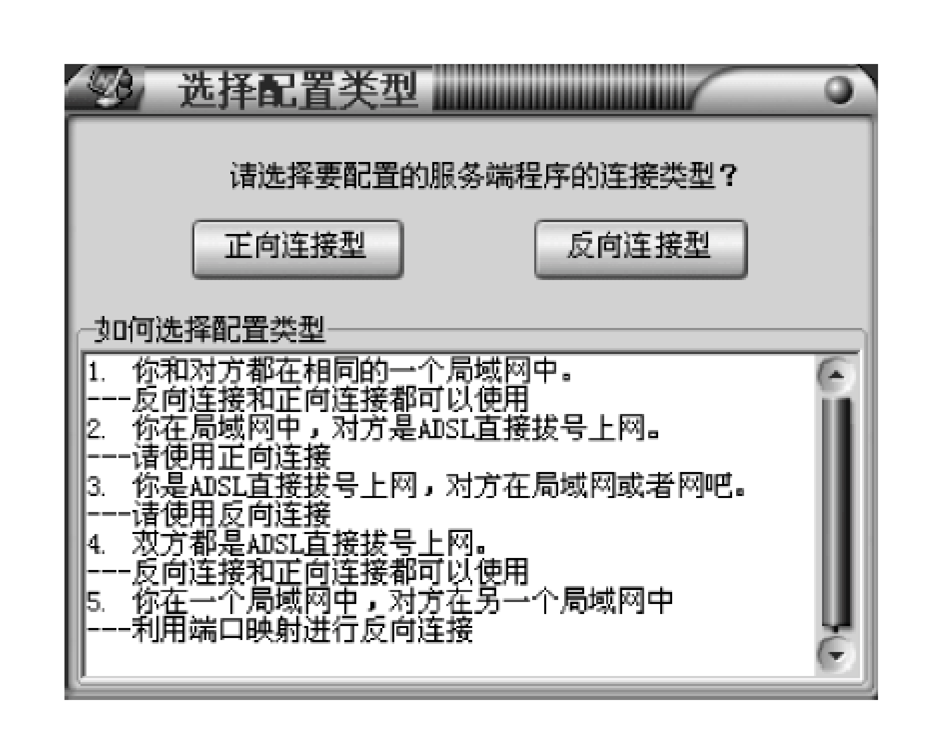


图 5-39 “选择配置类型”对话框(2)



图 5-40 “反向连接”对话框

③ 在“安装信息”选项卡中根据需要进行设置，如图 5-41 所示。

④ 设置完成后切换到“启动项目”选项卡，然后选中“远程主机是 Win9X 写入注册表启动项”和“远程主机是 2000/XP 注册为服务启动”复选框。在“服务启动项”组合框中，黑客通常会更改显示名称、服务名称及描述信息，以增强服务端的隐蔽性。在此保持默认设置，如图 5-42 所示。

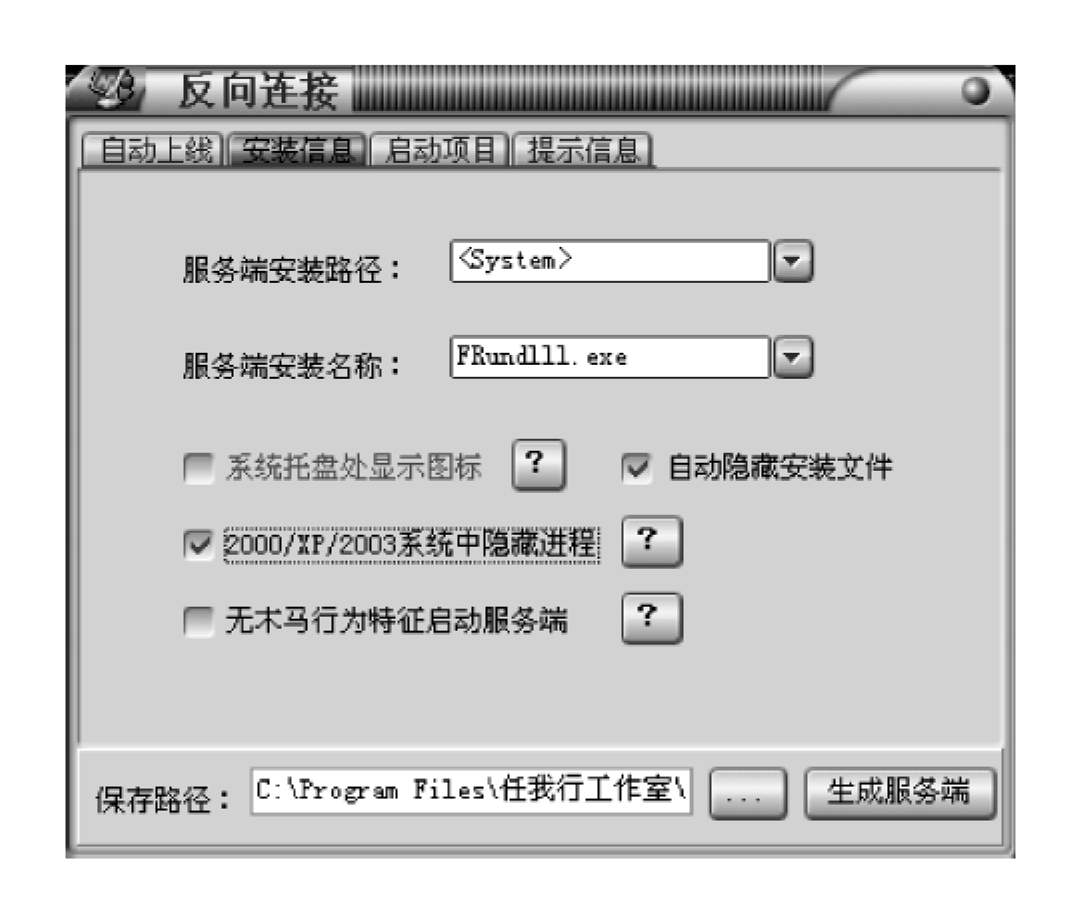


图 5-41 “安装信息”选项卡(2)

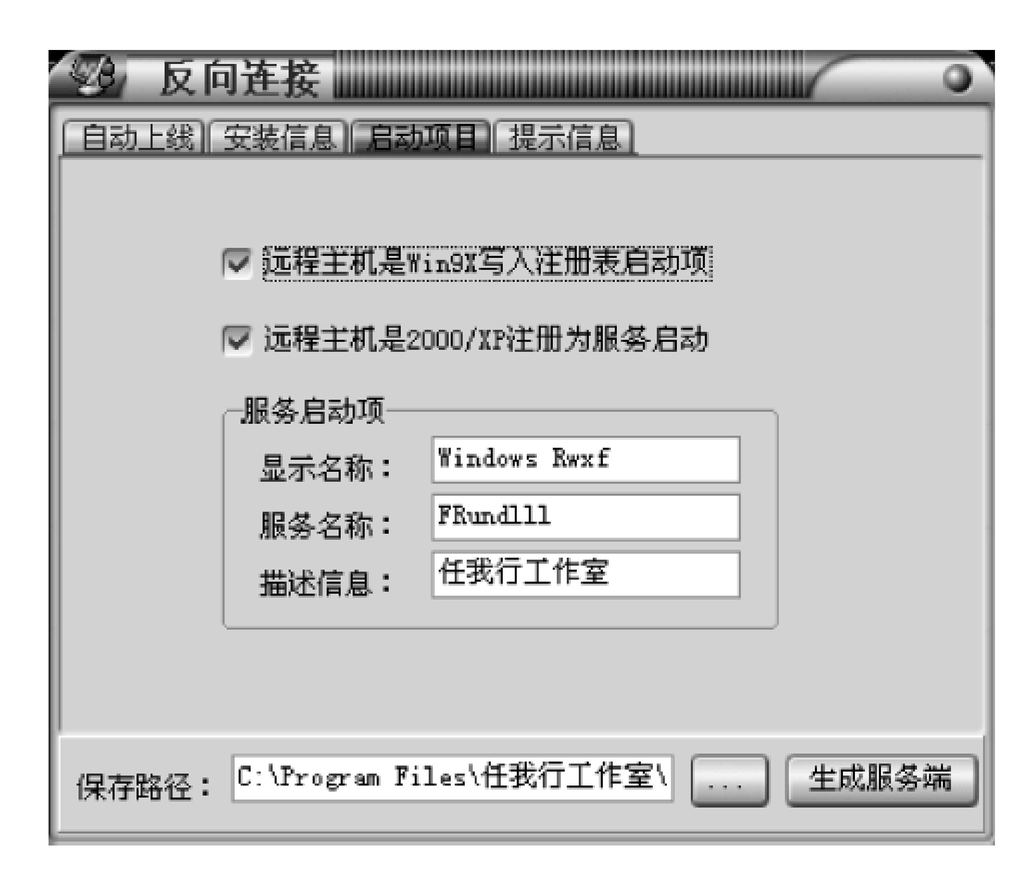


图 5-42 “启动项目”选项卡

⑤ 切换到“提示信息”选项卡，然后根据需要进行设置。设置完成后，在“反向连接”对话框底部的“保存路径”文本框中设置服务程序的保存路径，然后单击“生成服务端”按钮。反

向连接型服务端程序生成之后同样会打开一个提示对话框，单击“确定”按钮，如图 5-43 所示。

(3) 通过服务端程序进行远程控制

① 打开“任我行”程序主窗口，然后单击“正向连接”按钮。在“连接主机”文本框中输入局域网中被控主机的 IP 地址，然后单击窗口右侧的“连接”按钮。如果连接成功，在主窗口的底部会出现提示信息，如图 5-44 所示。

② 单击主窗口左侧窗格中“远程电脑”选项前面的“+”号，将展开被控计算机的磁盘分区。单击相应的磁盘分区，即可在右侧窗格中浏览到其中的文件内容，如图 5-45 所示。

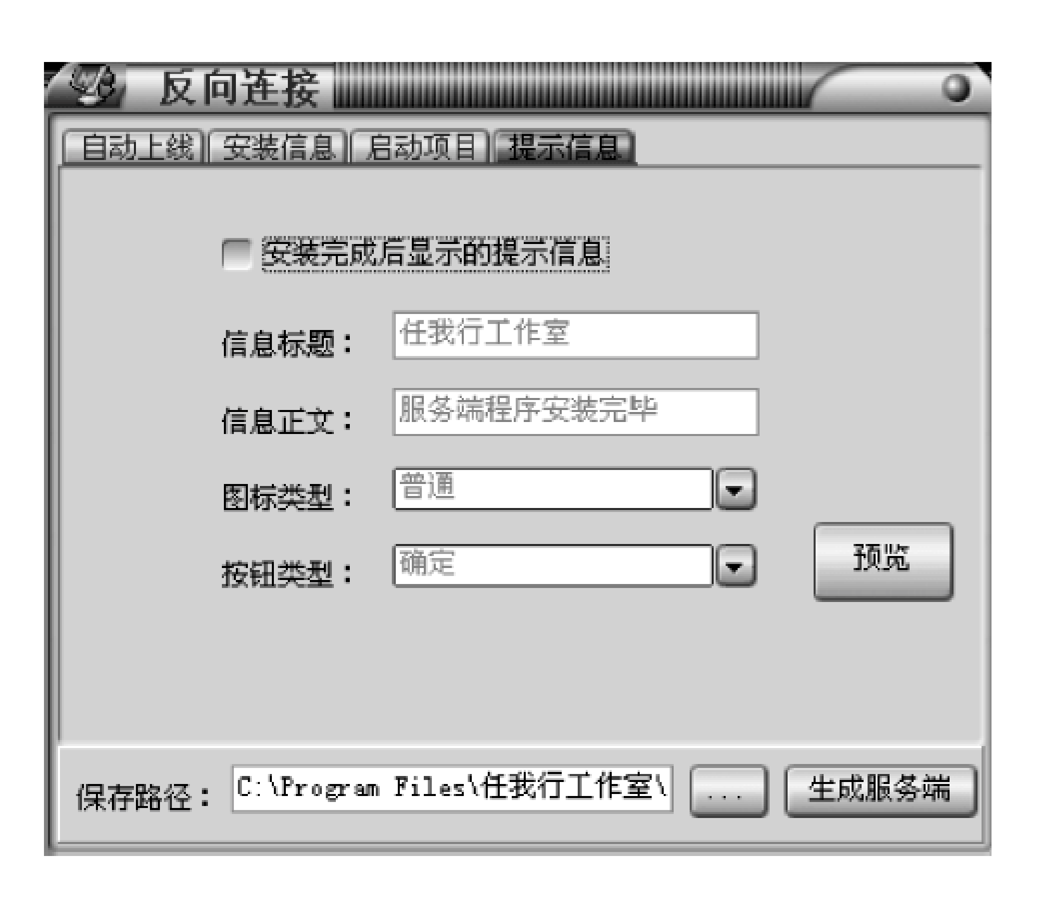


图 5-43　“提示信息”选项卡(3)



图 5-44　“任我行”程序主窗口

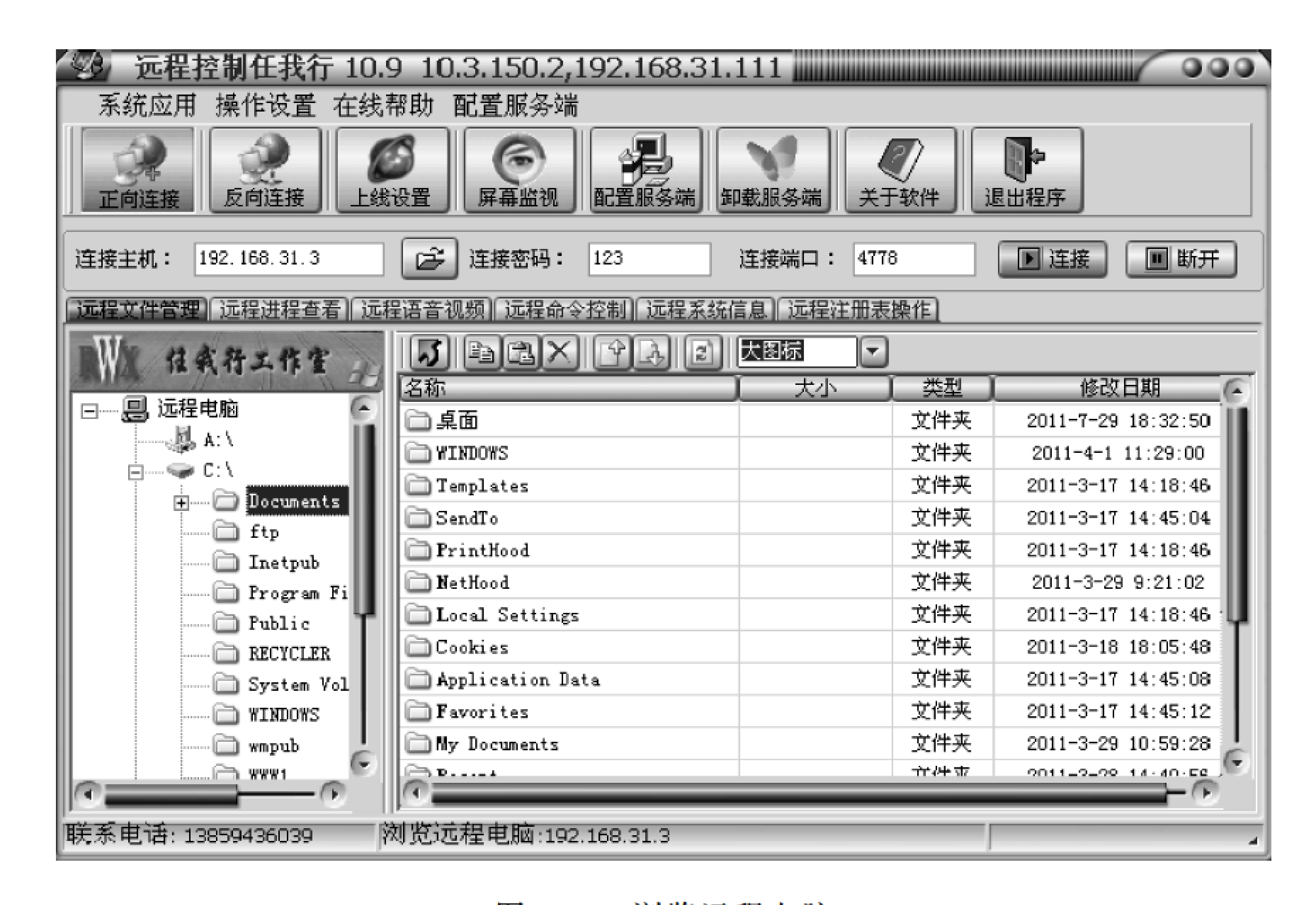


图 5-45　浏览远程电脑

③ 黑客若想将被控远程主机中的文件复制到自己的计算机中,可以选中需要复制的文件,然后右击,从弹出的快捷菜单中选中“文件下载”菜单项,如图 5-46 所示。

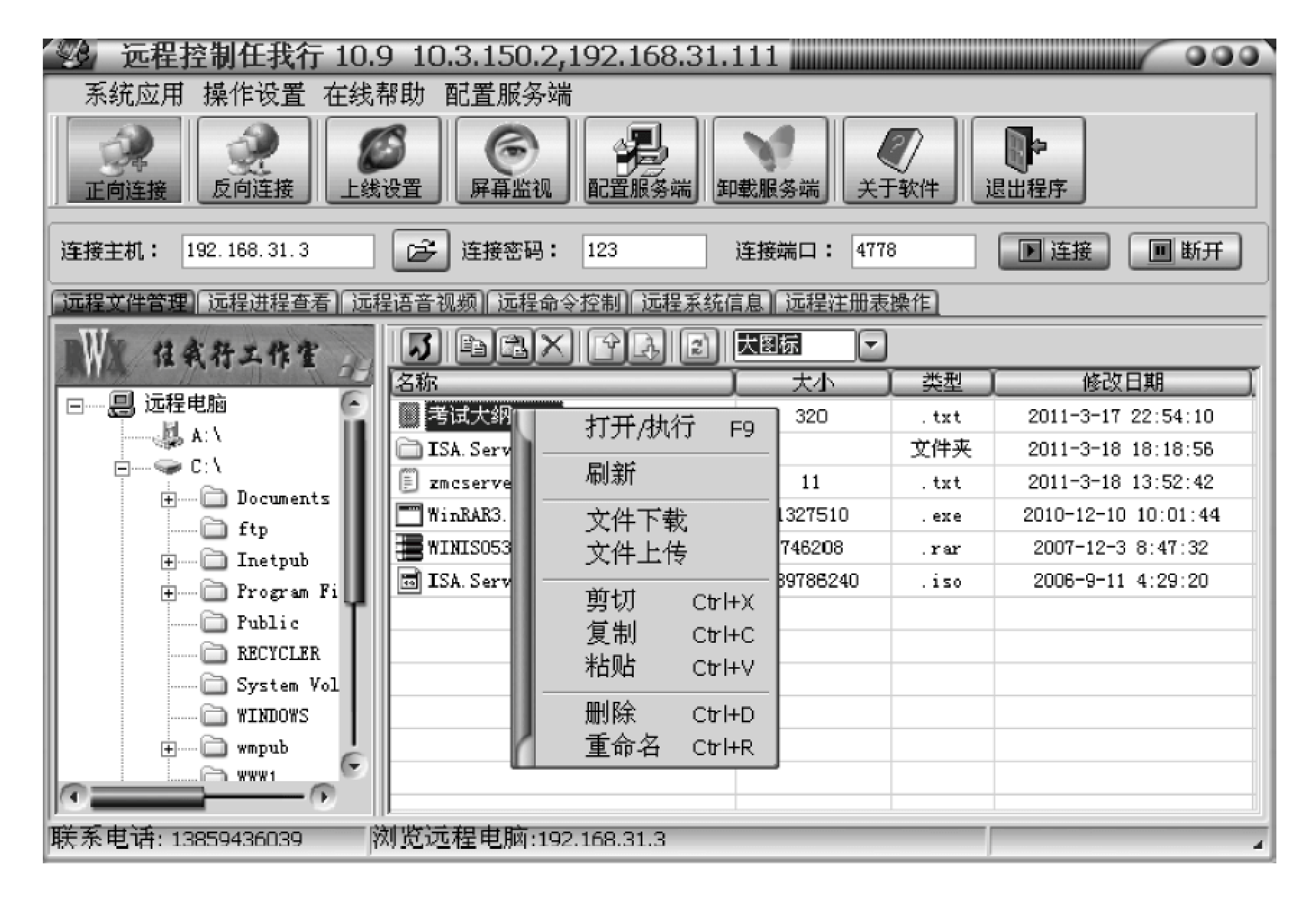


图 5-46 “文件下载”菜单项

④ 在弹出的“浏览文件夹”对话框中选中合适的存放位置,然后单击“确定”按钮,如图 5-47 所示。

⑤ 在弹出的“下载文件”对话框中单击“开始下载”按钮,文件便开始从远程主机下载,如图 5-48 所示。

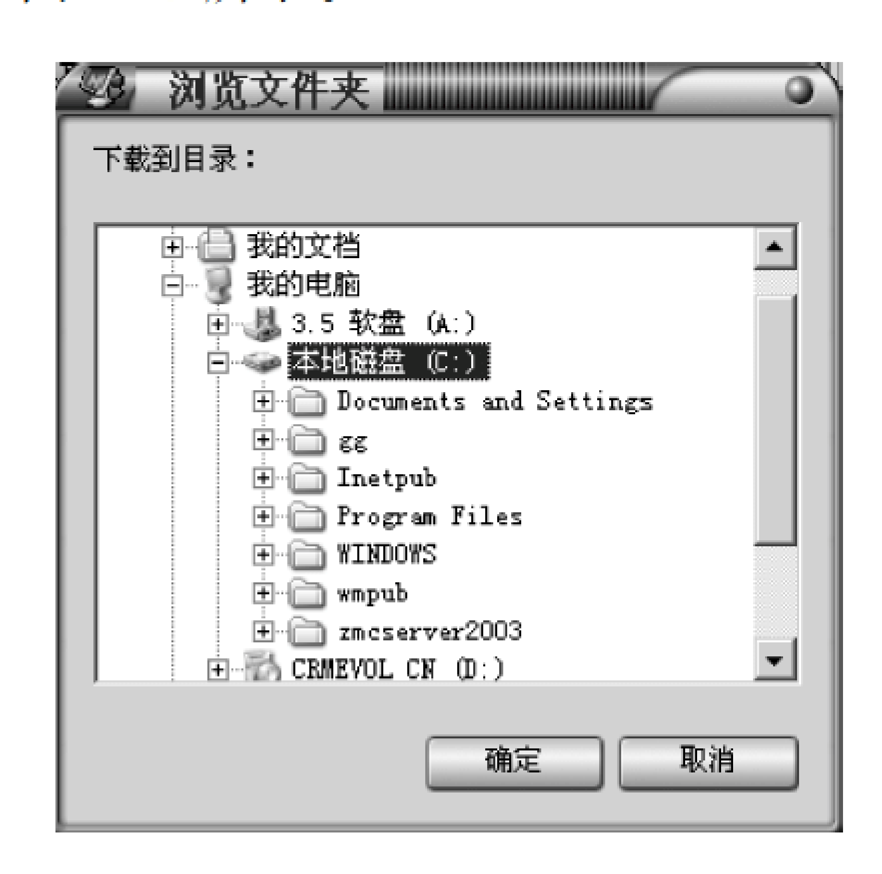


图 5-47 “浏览文件夹”对话框



图 5-48 “下载文件”对话框

⑥ 下载完成后,打开文件的存放路径可找到下载的文件。

⑦ 计算机被远程控制后,黑客会将木马程序放入被控计算机,方法是在被控计算机中找到要存放文件的位置,然后在“任我行”程序的主窗口右侧的窗格中右击,从弹出的快捷菜单中选择“文件上传”菜单项。

⑧ 在打开的“请选择上传文件”对话框中找到要上传的文件,然后单击“打开”按钮。在

打开的“上传文件”对话框中单击“开始上传”按钮，被选中的文件便会上传到远程被控计算机中的指定位置。

⑨ 如果黑客要删除远程被控主机中的文件，需在“任我行”程序主窗口的右侧窗格中找到并选中该文件，然后右击，从弹出的快捷菜单中选择“删除”菜单项。在打开的确认删除对话框中单击“确定”按钮，即可将该文件删除。

⑩ 如果想要查看远程被控主机中的进程，在“任我行”主窗口中切换到“远程进程查看”选项卡，可以看到远程计算机正在运行的进程，如图 5-49 所示。首次切换到该选项卡时，窗口中的显示是空白的，只需在窗口中的任意空白处右击，然后在弹出的快捷菜单中选择“刷新进程”命令，即可看到被控主机中的进程。此时，黑客可以设置被控主机各进程的优先级，还可以结束进程。



图 5-49 “远程进程查看”选项卡

⑪ 切换到“远程语音视频”选项卡，在“远程视频”区域单击“搜索”按钮后选择视频设备，然后单击“开启视频”按钮，可看到远程计算机摄像头抓取的视频。如果远程计算机上没有视频设备，则无法看到对方，如图 5-50 所示。



图 5-50 “远程语音视频”选项卡

⑫ 如果黑客要向被控计算机发送信息，可以在右侧的“发送信息”组合框中输入窗口标题和消息内容等信息，还可以设置图标类型和按钮类型。设置完成后单击“预览”按钮，可以

查看显示效果；单击“发送”按钮，可将消息发送给被控计算机。

⑬ 切换到“远程命令控制”选项卡，可以对远程计算机进行桌面图标控制、开/关机、死机黑屏以及改变声音等操作，如图 5-51 所示。



图 5-51 “远程命令控制”选项卡

⑭ 切换到“远程系统信息”选项卡，这里有“远程系统配置信息”、“远程剪贴板信息”、“远程运行窗体信息”3 个窗口，用户只要单击窗格下方的“查看”按钮，即可查看到该项信息。

⑮ 如果黑客想要查看远程系统的配置信息，需单击“远程系统配置信息”组合框中的“查看”按钮，如图 5-52 所示。

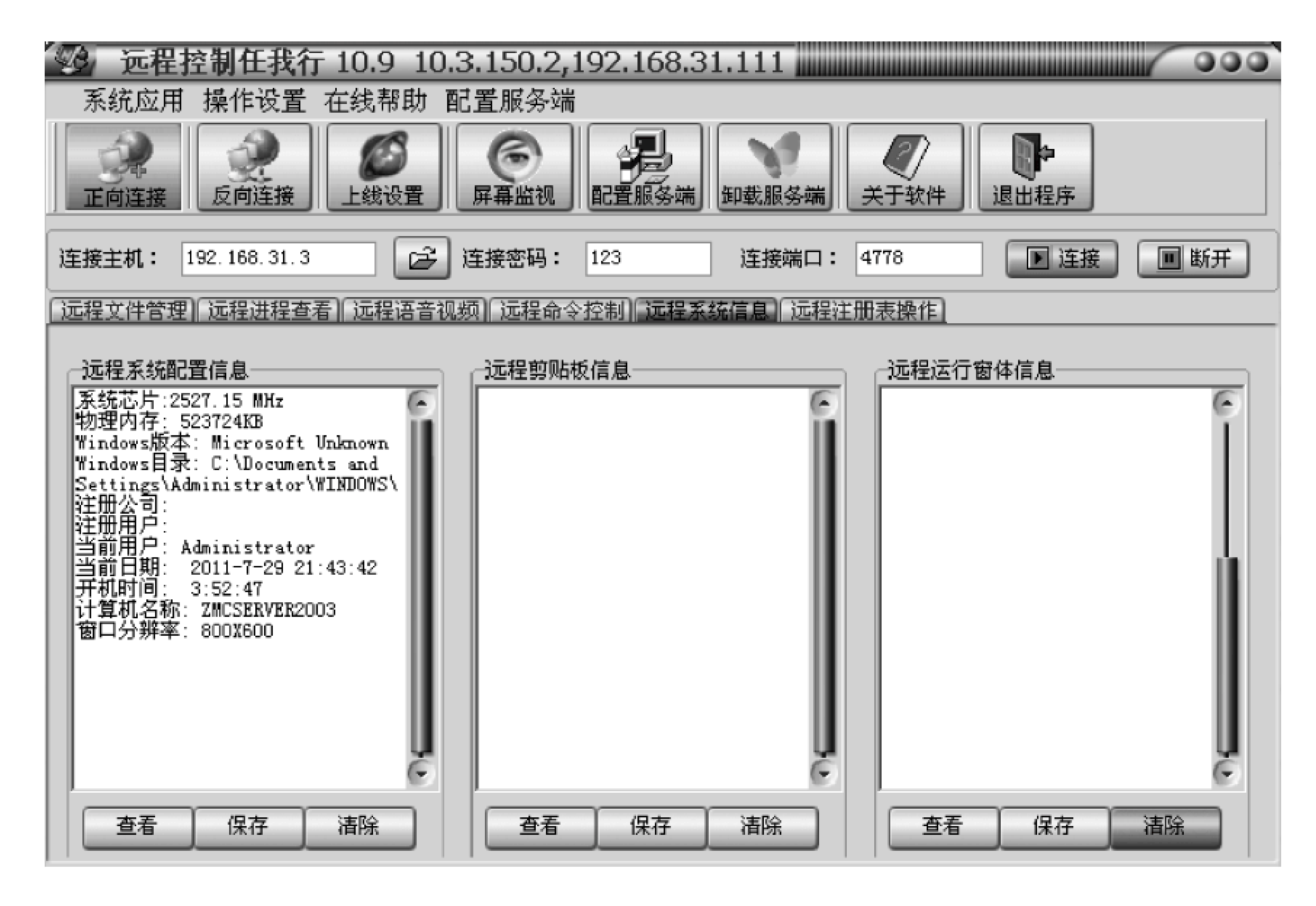


图 5-52 “远程系统配置信息”组合框

⑯ 如果黑客想要查看远程剪贴板中的信息,单击“远程剪贴板信息”组合框中的“查看”按钮即可,如图 5-53 所示。

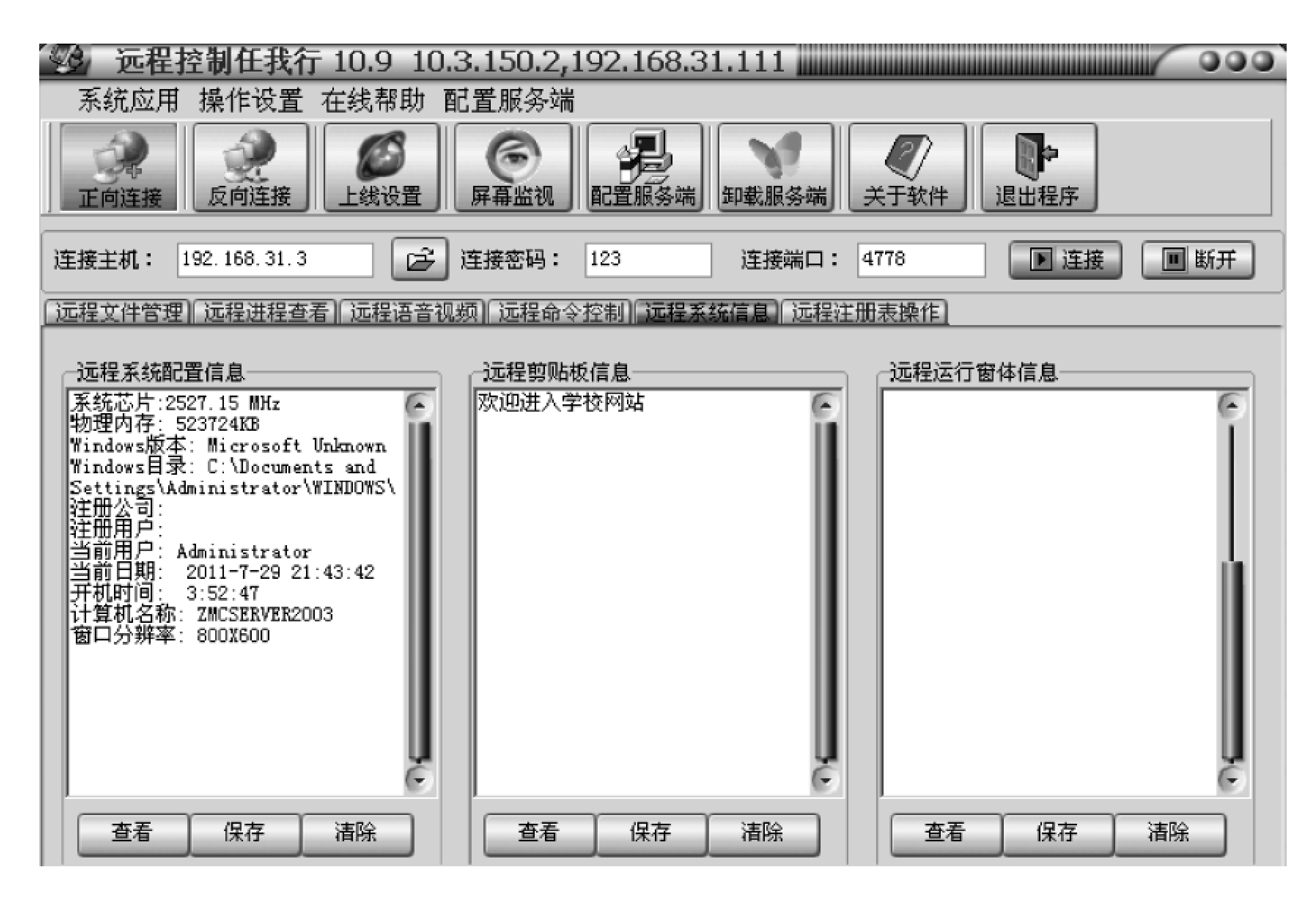


图 5-53　“远程剪贴板信息”组合框

⑰ 如果黑客想要查看远程运行窗体的信息,单击“远程运行窗体信息”组合框中的“查看”按钮即可,如图 5-54 所示。

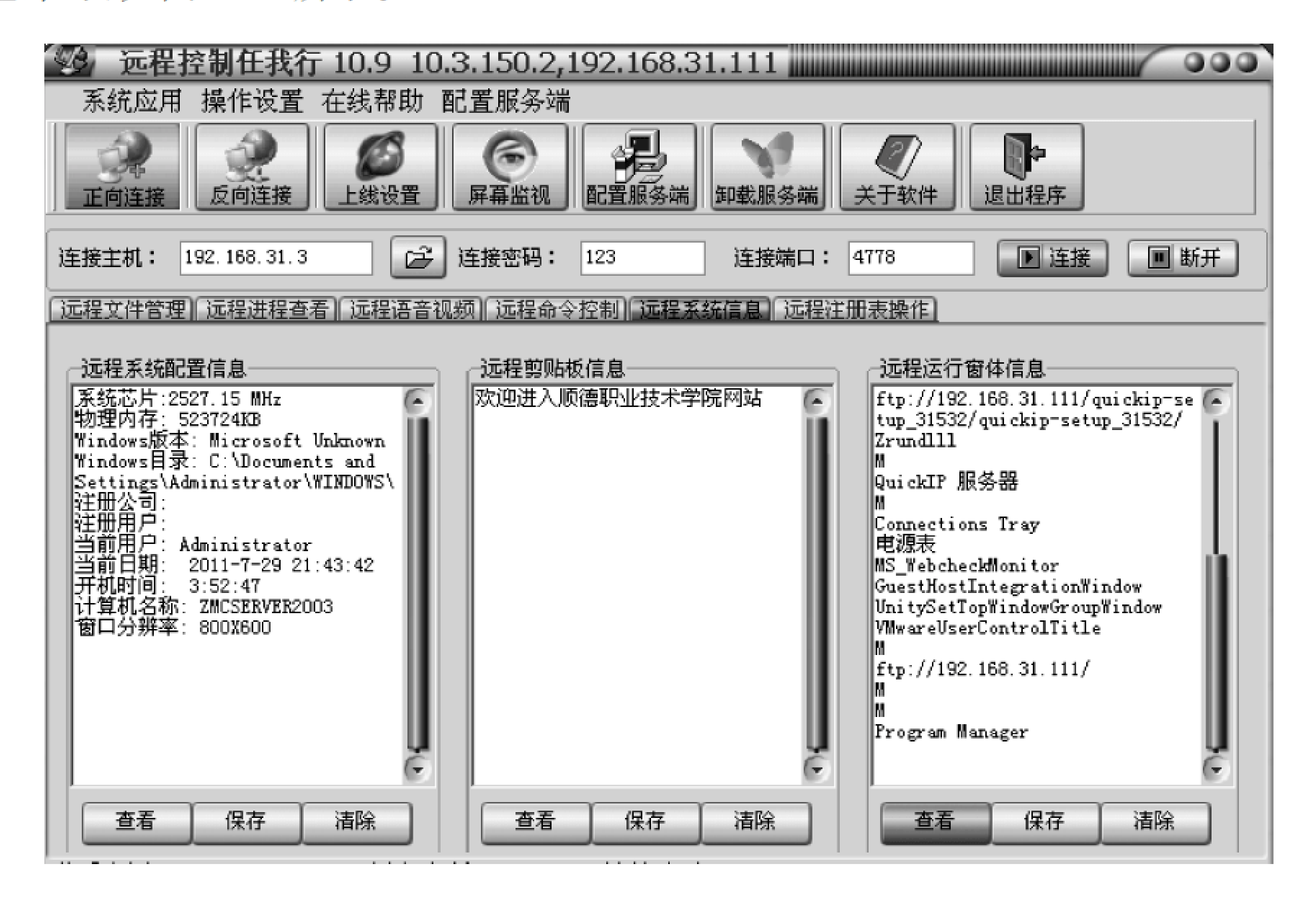


图 5-54　“远程运行窗体信息”组合框

⑱ 如果黑客想要对远程注册表进行操作,需切换到“远程注册表操作”选项卡,然后双击左侧窗格中的“远程电脑”选项,展开被控计算机的注册表。在此,黑客可以对注册表进行修改,如图 5-55 所示。



图 5-55 “远程注册表操作”选项卡

⑲ 如果黑客想要监视被控主机的屏幕,需单击主窗口中的“屏幕监视”按钮,弹出“屏幕监控-正向连接”窗口,然后单击窗口中的“连接”按钮,可看到被控计算机当前的界面内容。依次单击窗口中的“鼠标”和“键盘”按钮,即可使用自己的鼠标和键盘来控制对方计算机的鼠标与键盘操作。

⑳ 如果用户不想再监视该远程计算机,直接在“任我行”软件的工具栏中单击“卸载服务端”按钮即可。

5.5 常见问题解答

1. 被木马攻击的原因是什么?防御的措施有哪些?

答:被木马攻击的原因是开放了 IPC $ 连接和使用了弱口令。为了使自己的机器不成为“肉鸡”,应关闭 IPC $ 连接,关闭 139、445 端口,并使用复杂密码。

2. 为什么远程计算机已经正常运行了服务器端,却不能正常建立连接?

答:很多善意的远程控制软件都需要被控端操作者的确认,必须设置登录密码才能正确登录,这也是为了保证被控端计算机的安全。

3. 计算机病毒、恶意代码、网络蠕虫和木马的区别与联系是什么?

答:计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能,或者毁坏数据以影响计算机使用,并能自我复制的一组计算机指令或代码。传染性是判断一段程序代码是否为计算机病毒的依据。网络病毒的主要特征包括传播方式多样、传播速度极快、影响面极广、破坏性极强、难以控制和根治、编写方式多样,病毒变种多、智能化,兼有木马、蠕虫和后门等功能。恶意代码是指在不被察觉的情况下,把代码寄宿到另一段程序中,进而通过运行有入侵性或破坏性的程序,达到破坏被感染计算机和网络系统的目的。恶意代码包括普通病毒、蠕虫、木马等。网络蠕虫是一个自我包含的程序,它能够传播自身的功能或复制自

身的片段到其他与网络连通的计算机系统。网络蠕虫由多个部分组成,每个部分运行在不同计算机上,并使用网络进行通信。与计算机病毒不同,蠕虫不需要把自身附加在宿主程序上,而是一个独立的程序,能够主动运行。木马与病毒的不同之处在于,木马是没有自我复制功能的恶意程序。

5.6 过关练习

一、选择题

1. 计算机感染特洛伊木马后的典型现象是(　　)。

   A. 程序异常退出　　B. 有未知程序试图建立网络连接

   C. 邮箱被垃圾邮件填满　　D. Windows 系统黑屏

2. 下列行为不属于网络攻击的是(　　)。

   A. 连续不断 ping 某台主机　　B. 发送带病毒和木马的电子邮件

   C. 向多个邮箱群发送一封电子邮件　　D. 暴力破解服务器密码

3. 在下面 4 种病毒中,(　　)可以远程控制网络中的计算机。

   A. worm. Sasser. f　　B. Win32. CIH

   C. Trojan. qq3344　　D. Macro. Melissa

二、实操题

在自己和朋友的计算机上使用软件试着进行远程控制。

工作任务六

拒绝服务攻击

6.1 用户需求与分析

拒绝服务攻击利用合理的服务请求来占用过多的服务资源，从而使合法用户无法及时得到服务响应。攻击者进行拒绝服务攻击，实际上是让服务器实现两种效果，一种是迫使服务区的缓冲区满，不能接收新的请求；另一种是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。

6.2 预备知识

6.2.1 拒绝服务攻击的定义

拒绝服务攻击简称 DoS，是英文 Denial of Service 的缩写。拒绝服务攻击的方式有很多，最基本的是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。拒绝服务攻击的目的是为了让目标主机停止提供服务或资源访问，这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。

拒绝服务攻击的方式有多种，根据攻击的手法和目的的不同，可以分为两种。一种拒绝服务攻击以消耗目标主机的可用资源为目的，使目标主机疲于应付大量无用的连接请求，占用了所有的资源，无法对正常的请求作出及时响应，从而导致服务中断。这种攻击主要利用网络协议或系统漏洞进行攻击，主要的攻击方式有死亡之 ping、SYN Flood、UDP Flood、ICMP Flood、Land 等。另一种拒绝服务攻击以消耗目标主机的有效带宽为目的，攻击者通过发送大量数据包，将整条链路的带宽全部占用，从而使合法用户请求无法通过链路到达目标主机。例如，蠕虫对网络的影响。具体的攻击方式有发送垃圾邮件，向 FTP 服务器塞垃圾文件，塞满目标主机的硬盘，伪装账号错误登录，导致账号连续多次登录失败而被锁定，那么正常的合法用户也不能用这个账号登录系统了。

6.2.2 常见拒绝服务攻击行为及防御方法

下面针对几种典型的拒绝服务攻击行为进行分析，并提出相应的对策。

1. 死亡之 ping(Ping of Death)攻击

早期，路由器对数据包的大小有限制，很多操作系统的 TCP/IP 规定 ICMP 包的大小限制在 64KB 以内。遇到超过 64KB 的 ICMP 包，会出现内存分配错误，使接收方计算机死机。根据这一原理，黑客们只需要不断地通过 ping 命令向攻击目标发送超过 64KB 的数据

包,就可以使接收方计算机死机。

防御的方法是使用补丁程序,在接收数据包之前先判断数据包的大小是否大于64KB,超过则丢弃该数据包。现在所有的TCP/IP协议都具有对付超过64KB数据包的处理能力,并且大多数防火墙能自动过滤这些攻击。很多操作系统,如Windows XP/Server 2003、Linux等都具有抵抗一般死亡之ping的能力。

2. 泪滴(Teardrop)攻击

对于一些大的数据包,为了符合链路层最大传输单元(MTU)的要求,往往需要拆分传送。这样,接收端在接收完全部IP数据包后,可以根据"偏移字段"得知某个片段在整个IP包中的位置,从而将这些片段重新组装。如果黑客在截取IP数据包后,把"偏移字段"设置成错误的值,导致接收端不能正确组合这些拆分的数据包,但接收端会不断尝试,就导致目标主机因资源耗尽而崩溃。

防御方法是对接收到的分片数据包进行分析,计算数据包的片偏移量是否有误。反攻击的方法是添加系统补丁程序,丢弃收到的病态分片数据包,尽可能采用最新的操作系统,或在防火墙上设置分段重组功能,由防火墙接收同一原包中的所有拆分数据,然后完成重组工作。

3. TCP SYN洪水(TCP SYN Flood)攻击

攻击者利用伪造的IP地址向目标主机发出多个连接(SYN)请求,目标主机在接收到请求后发送确认信息,并等待回答。由于IP地址是伪造的,所以确认信息也不会到达任何计算机,当然不会有任何计算机为此确认信息作出应答。而在没有收到应答之前,目标计算机会在缓冲区保持连接信息并一直等待。当等待连接达到一定数量,缓冲区资源耗尽后,开始拒绝所有其他连接请求,当然也包括本来属于正常应用的请求。

防御方法是检查单位时间内收到的SYN连接是否超出系统设定的值。当接收到大量SYN数据包时,通知防火墙阻断连接请求或丢弃数据包,并在防火墙上过滤来自同一主机的后续连接。由于此类攻击不寻求响应,所以无法将其从一个简单的高容量传输中鉴别出来。

4. Land攻击

Land攻击中的数据包源地址和目标地址是相同的。当操作系统收到这类数据包时,不知该如何处理,循环发送和接收该数据包会消耗大量的系统资源,有可能造成系统崩溃或者死机。

防御的方法是直接通过判断网络数据包的源地址和目标地址是否相同来确认是否属于攻击行为。反攻击的方法是配置防火墙设备或制定包过滤路由器的包过滤规则。

5. 分片IP报文攻击

攻击者给目标主机只发送一片分片报文,而不发送所有的分片报文,目标主机便会一直等待;如果攻击者发送了大量分片报文,会消耗掉目标主机的资源,导致不能接收正常的IP报文。

对于这种攻击方式,目前还没有十分有效的防御方法。对于一些包过滤设备或入侵检测系统来说,通常是通过判断第一个分片的目标端口号来决定后续分片是否允许通过,但一些恶意分片的目标端口号位于第二个分片中,会躲过一些入侵检测系统及安全过滤系统,从

而在目标主机上重组之后形成各种攻击。目前有一些智能的包过滤设备可以直接丢掉报头中不包含端口信息的分片,但这种设备价格较高,不是每个企业都能承受得起的。

6. Smurf 攻击

利用多数路由器具有同时向许多计算机广播请求的功能,攻击者伪造一个合法的 IP 地址,然后由网络上所有的路由器广播要求向受攻击计算机地址作出回答的请求。由于这些数据包看上去是来自已知地址的合法请求,使得网络中所有主机都对此 ICMP 应答请求作出答复,导致网络阻塞。这种攻击比“死亡之 ping”和“SYN 洪水”流量高出 1～2 个数量级,更容易攻击成功。还有些 Smurf 攻击将源地址改成第三方受害者的 IP 地址,而不是伪造的 IP 地址,最终导致第三方受害者计算机系统崩溃。

防御的方法是关闭外部路由器或防火墙的广播地址特性,并在防火墙上设置规则,丢弃 ICMP 协议类型的数据包。

7. 虚拟终端(VTY)耗尽攻击

交换机和路由器等网络设备为了便于远程管理,一般都设置了 Telnet 用户界面,即用户可以通过 Telnet 远程登录到该设备上,对这些设备进行管理。通常,这些设备的 Telnet 用户界面个数是有限制的,比如 5 个或 10 个。然而,攻击者同时跟一个网络设备建立 5 个或 10 个 Telnet 连接,会导致这些设备的远程管理界面被占尽,当合法用户再对这些设备进行远程管理时,会因为 Telnet 连接资源被占用而失败。

防御的方法是升级交换机和路由器等网络设备的 COS 或 IOS 系统,新版本的系统已经对该问题进行了改进。

8. 电子邮件炸弹

攻击者在很短的时间内连续不断地向同一地址发送大量电子邮件,耗尽邮件接收者的网络带宽资源,导致网络拥塞,使大量合法用户不能正常工作；同时占用邮件接收者有限的邮箱容量,用户的邮箱将没有多余的空间接纳新邮件,新邮件将会丢失或退回,造成邮箱失效；而邮件炸弹携带的大容量信息不断在网络中来回传输,堵塞传输信道,加重邮件服务器的工作强度,减缓处理其他用户电子邮件的速度,导致恶性循环。

防御的方法是对邮件进行过滤,自动删除来自同一主机的过量或重复的消息；或在接收任何电子邮件之前预先检查发件人的资料,有可疑之处便将其删除；同时,将邮件服务器设置为自动删除超过信箱容量的大邮件,以有效避免“中弹”。

6.2.3 分布式拒绝服务攻击的定义

分布式拒绝服务攻击(Distributed Denial of Service,DDoS)又称为洪水攻击。它是一种分布、协作的大规模攻击方式,攻击者利用多台计算机攻击比较大的商业站点、搜索引擎、政府部门站点等。DDoS 是在传统的 DoS 的基础上发展起来的一类攻击方式。单一的拒绝服务攻击一般采用一对一的方式,当攻击目标的 CPU 速度、内存或网络带宽等各项性能指标不高时,这种攻击的效果较明显。随着计算机与网络技术的发展,计算机的处理能力迅速增强,内存大大增加,网络带宽也越来越大,对于恶意攻击包的“消化能力”增强了不少,使得 DoS 攻击的困难程度增加了。这时,分布式拒绝服务攻击应运而生。当计算机和网络的处理能力增强时,用一台计算机攻击不再有效,那么攻击者采用分布式、协同式的大规模攻击

方式,利用多台计算机来发起攻击,以比以前更大的规模来进攻目标主机。

6.3 方案设计

方案设计如表 6-1 所示。

表 6-1 方案设计

任务名称	拒绝服务攻击
任务分解	1. 拒绝服务攻击工具 SYN Flood 的使用 2. 分布式拒绝服务攻击工具 DDoS 攻击者的使用
能力目标	1. 能对拒绝服务攻击工具 SYN Flood 的攻击属性进行设置 2. 能使用拒绝服务攻击工具 SYN Flood 对目标主机发动拒绝服务攻击 3. 能使用网络监听工具查看攻击效果 4. 能对分布式拒绝服务攻击工具 DDoS 攻击者的攻击属性进行设置 5. 能使用分布式拒绝服务攻击工具 DDoS 攻击者对目标主机发动拒绝服务攻击
知识目标	1. 熟悉拒绝服务攻击的定义 2. 了解拒绝服务攻击的原理 3. 了解常见拒绝服务攻击的行为及防御方法
素质目标	1. 培养良好的职业道德 2. 树立较强的安全意识 3. 掌握网络安全行业的基本情况 4. 树立较强的安全、节约、环保意识

6.4 任务实施

6.4.1 任务 1:拒绝服务攻击工具 SYN Flood 的使用

1. 任务目标

使用 SYN Flood 伪造源 IP 地址、源端口号,对目标主机发动攻击。攻击类型包括 SYN、PSH&ACK、3HD、Rage3HD、ICMP、碎片 SYN、WebTest。

2. 工作任务

拒绝服务攻击工具 SYN Flood 的攻击。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机,通过网络相连。

(2) 软件工具:拒绝服务工具 SYN Flood。

4. 实施过程

(1) 双击 SYN Flood 运行程序,弹出主程序窗口。单击“新建攻击”按钮,弹出“攻击属性设置”对话框,如图 6-1 所示。

(2) 在“攻击属性设置”对话框中填入攻击目标的 IP 地址,然后选择攻击类型,比如

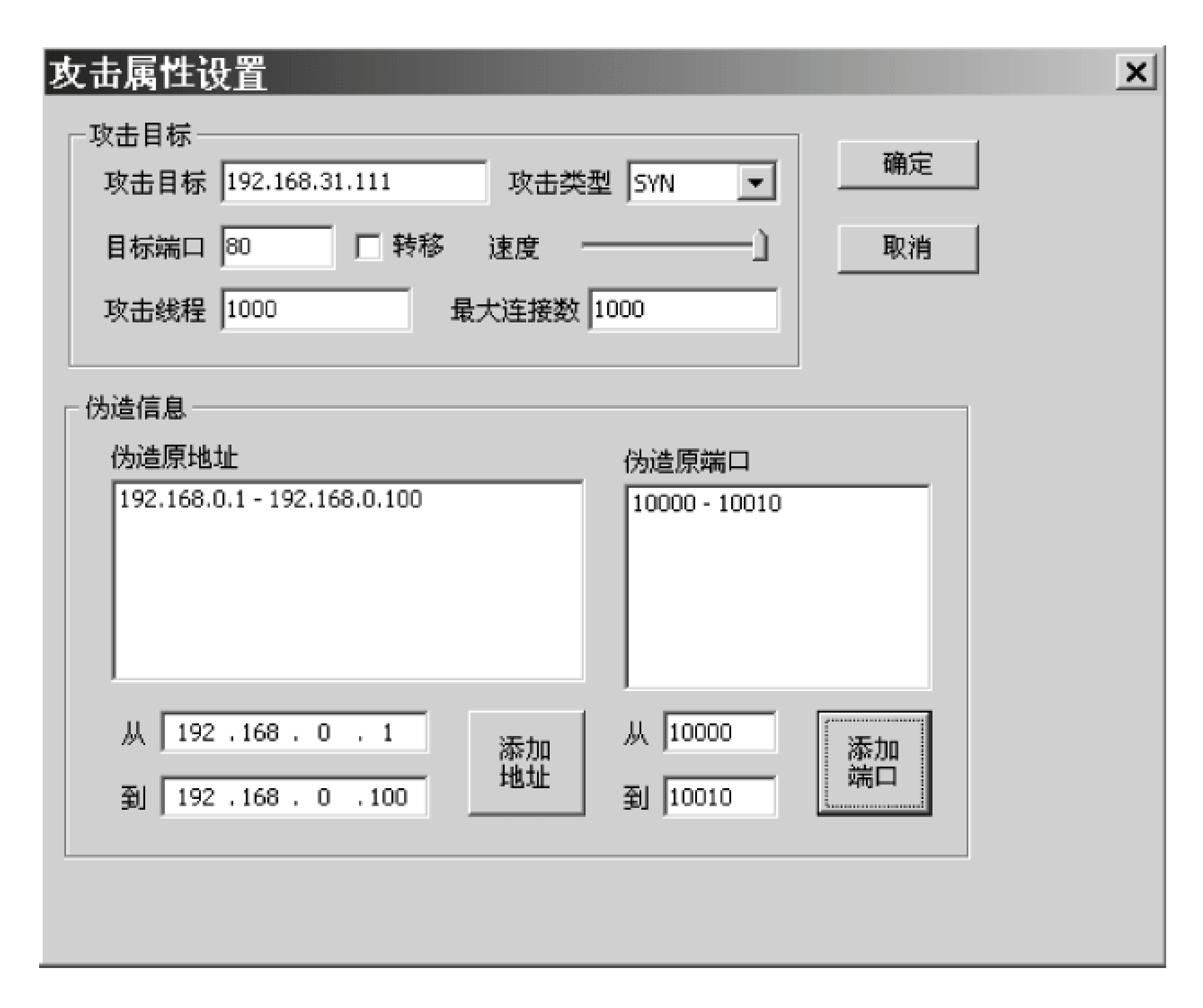


图 6-1 “攻击属性设置”对话框

“SYN”,再设置目标端口、攻击线程和最大连接数,添加伪造原地址和伪造原端口范围,并单击“确定”按钮。

(3) 被攻击的目标主机通过 Sniffer Pro 查看到网络连接情况,发现有 100 台主机与目标主机相连,如图 6-2 所示。

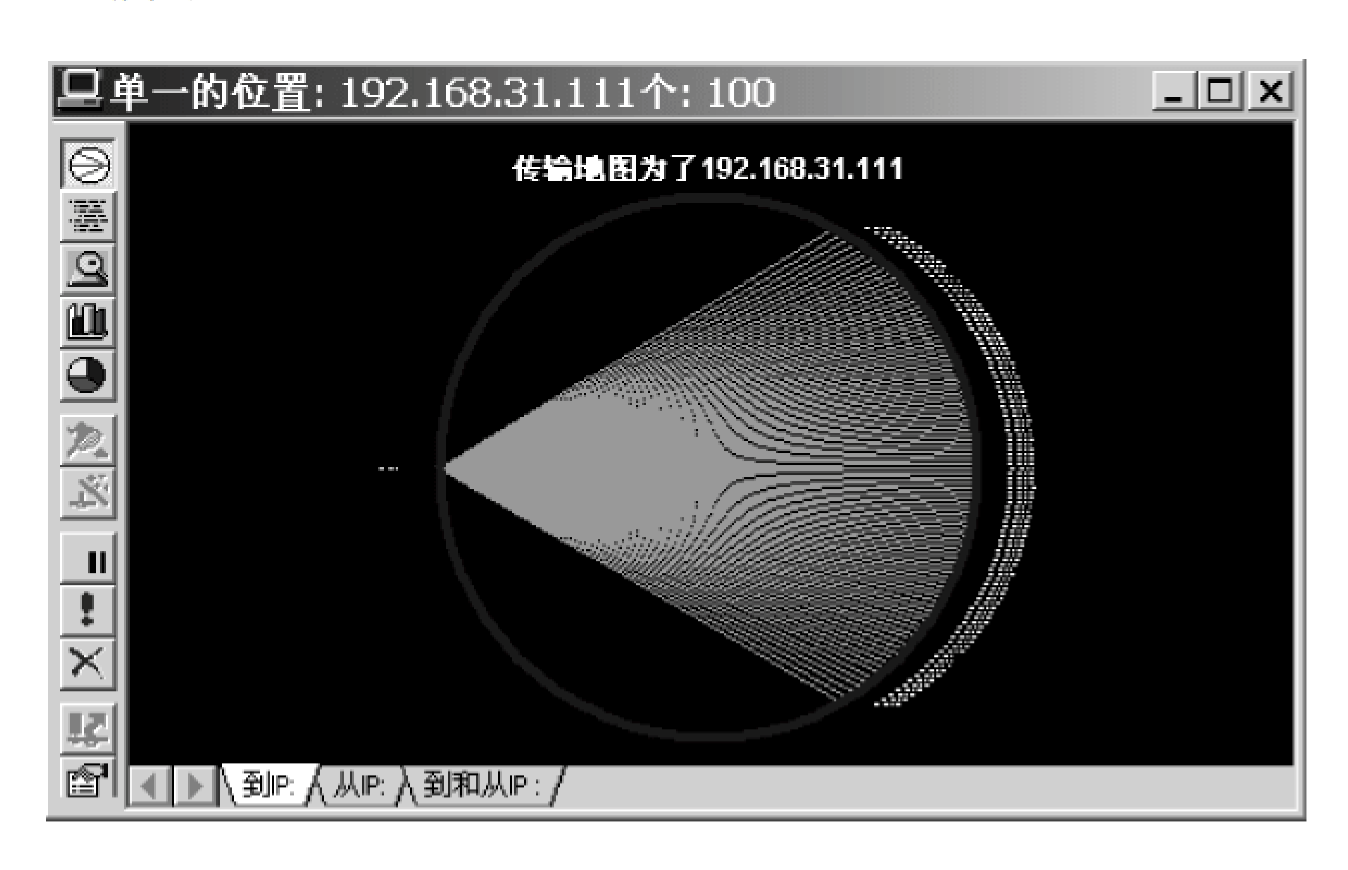


图 6-2 目标主机的网络连接示意图

(4) 还可以查看到整个网络中计算机所用带宽前 10 名的情况,如图 6-3 所示,都是由伪装 IP 地址发送的数据包。

(5) 通过任务管理器观察系统性能的变化,CPU 利用率从 10%上升到 100%,可以看到 SYN Flood 攻击的危害性,如图 6-4 所示。

(6) 这是一对一攻击的结果。如果是多对一攻击,会导致被攻击主机蓝屏。在攻击端主窗口单击“新建攻击”按钮,可以添加攻击线程,增强攻击效果。

(7) 在攻击端主窗口单击“退出”按钮结束攻击。

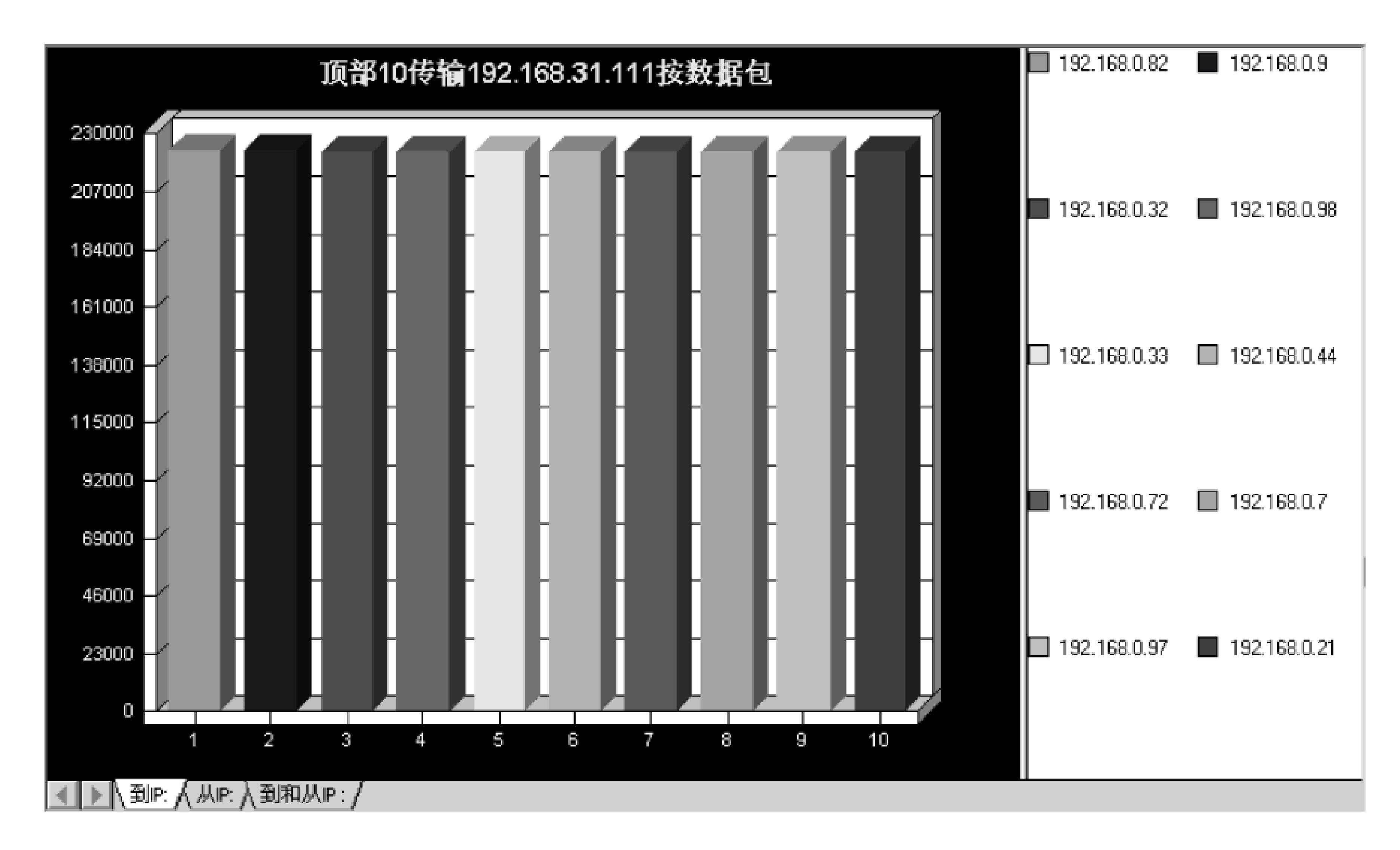


图 6-3　网络中带宽显示柱状图



图 6-4　SYN 攻击后的系统性能变化

6.4.2　任务 2：分布式拒绝服务攻击工具 DDoS 攻击者的使用

1. 任务目标

本软件是一个 DDoS 攻击工具。程序运行后自动驻入系统，并在以后随系统启动，在上网时自动对事先设定好的目标进行攻击。可以自由设置“并发连接线程数”、“最大 TCP 连接数”等参数。由于采用了与其他同类软件不同的攻击方法，效果更好。

2. 工作任务

分布式拒绝服务攻击工具 DDoS 攻击测试。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机,通过网络相连。

(2) 软件工具:DDoS 攻击测试工具。

4. 实施过程

(1) 运行 DDoS 攻击生成器(DDoSMaker.exe),弹出"DDoS 攻击者 生成器"对话框,如图 6-5 所示。

(2) 进行必要的设置:在"目标主机的域名或 IP 地址"文本框中填入要攻击主机的域名或 IP 地址;在"端口"文本框中填入要攻击的端口,这里需要填 TCP 端口,因为该工具只能攻击基于 TCP 的服务,填入"80"攻击 HTTP 服务,填入"21"攻击 FTP 服务,填入"25"攻击 SMTP 服务,填入"110"攻击 POP3 服务;"并发连接线程数"是指同时有多少个线程去连接指定的端口,此值越大,对目标主机的攻击越强,但占用本机资源越大,默认值是 10 个线程;"最大 TCP 连接数"的默认值是 1000 个连接;最后,在"DDoS 攻击者程序保存为"文本框内指定生成的 DDoS 攻击者程序保存的位置和名称。

(3) 双击生成的 DDoS 攻击者程序,开始对目标主机发起攻击。

(4) 通过目标主机的任务管理器观察系统性能的变化,从 CPU 利用率变化可以看到 DDoS 攻击的危害性,如图 6-6 所示。



图 6-5 "DDoS 攻击者 生成器"对话框

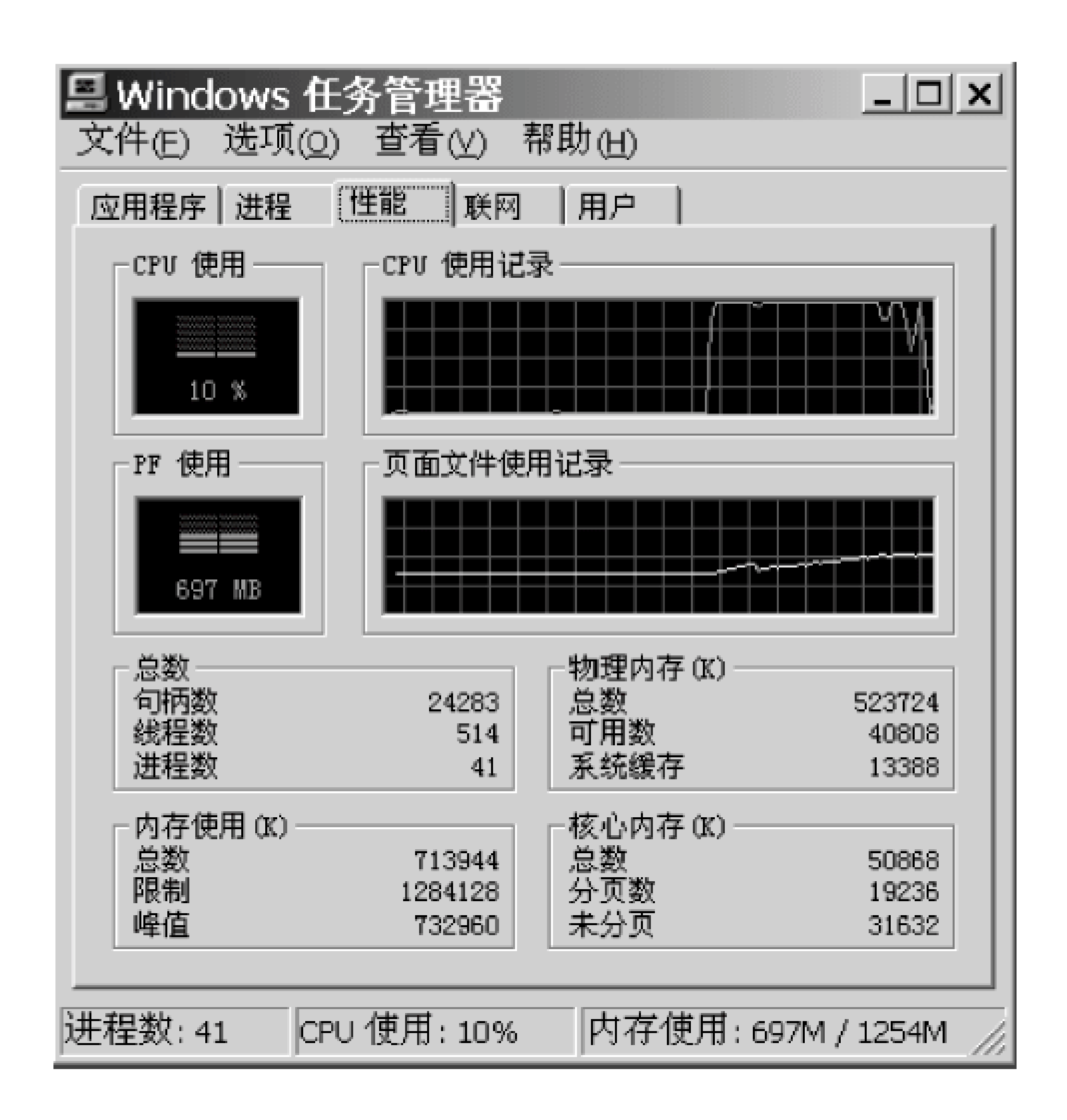


图 6-6 任务管理器

6.5 常见问题解答

1. DoS 攻击和 DDoS 攻击的区别是什么?

答:DoS 是一种利用单台计算机的攻击方式;DDoS 是一种基于 DoS 的特殊形式的拒绝服务攻击,是一种分布、协作的大规模攻击方式,主要瞄准比较大的站点,如商业公司、搜索引擎和政府部门的站点。DDoS 攻击是利用一批受控制的计算机向一台计算机发起攻击,这样来势凶猛的攻击让人难以防备,因此具有更大的破坏性。

2. 防御 DDoS 攻击的方法有哪些？DDoS 攻击是不是可以 100%防御的？

答：防御 DDoS 攻击是一个系统工程，仅仅依靠某种系统或产品来防御是不现实的，100%完全杜绝 DDoS 攻击在目前是不可能的，但通过适当的措施抵御 90%的 DDoS 攻击还是可以做到的。防御 DDoS 攻击的方法有：定期扫描，在骨干节点配置防火墙，用足够的计算机承受黑客攻击，充分利用网络设备保护网络资源，以及过滤不必要的服务和端口。基于攻击和防御的成本开销考虑，如果通过适当的措施增强了抵御 DDoS 的能力，意味着增大了攻击者的攻击成本，那么绝大多数攻击者都将因无法继续下去而放弃，相当于成功地抵御了 DDoS 攻击。

6.6 过关练习

一、选择题

1. 拒绝服务攻击(　　)。

A. 用超出被攻击目标处理能力的海量数据包消耗可用系统、带宽资源等
B. 全称是 Distributed Denial of Service
C. 拒绝来自一台服务器发送回应请求的指令
D. 入侵控制一台服务器后远程关机

2. “TCP SYN Flood”建立大量处于半连接状态的 TCP 连接，其攻击目标是网络的(　　)。

A. 保密性　B. 完整性　C. 真实性　D. 可用性

3. 当感觉到操作系统运行速度明显减慢，打开“任务管理器”后发现 CPU 的使用率达到 100%时，最有可能受到(　　)攻击。

A. 特洛伊木马　B. 拒绝服务　C. ARP　D. 网络监听

4. 在网络攻击活动中，Tribal Flood Network(TFN)是(　　)类的攻击程序。

A. 拒绝服务　B. 字典攻击　C. 网络监听　D. 病毒程序

5. (　　)无法有效防御 DDoS 攻击。

A. 根据 IP 地址对数据包进行过滤
B. 为系统访问提供更高级别的身份认证
C. 安装防病毒软件
D. 使用工具软件检查不正常的高流量

6. DDoS 攻击破坏了网络的(　　)。

A. 可用性　B. 保密性　C. 完整性　D. 真实性

7. 驻留在多个网络设备上的程序在短时间内同时产生大量的请求消息冲击某 Web 服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这属于(　　)。

A. 上网冲浪　B. 中间人攻击　C. DDoS 攻击　D. MAC 攻击

二、操作题

对本地计算机进行 SYN 攻击压力测试。

学习情境二

企业网中常见防护技术分析

本学习情境主要介绍防护技术，即操作系统日常维护中最重要的内容，包括系统账户的管理、注册表的管理与维护、系统进程和服务的管理、Internet 信息服务的安全管理等。以5个工作任务为案例，除了介绍系统内置的管理工具外，还介绍实际工作中常用的加密工具PGP 的使用方法，来进一步加强操作系统的安全管理。

学生通过本单元所有任务的实践，可以学会如何对企业网操作系统进行安全部署，解决系统平台配置中遇到的网络安全问题，学习账户管理、注册表管理、进程和服务管理所需要的相关网络安全知识，能排除网络中可能出现的问题，为将来工作积累实践经验。

本学习情境需要完成的工作任务如下：

工作任务七　系统的账户管理
工作任务八　注册表的管理
工作任务九　组策略的设置
工作任务十　数据加密技术的使用
工作任务十一　Internet 信息服务的安全设置

工作任务七

系统的账户管理

7.1 用户需求与分析

黑客在不知道系统管理员密码的情况下,可以通过多种手段破解系统管理员账户的密码,如果没有采取必要的防范措施,会严重影响用户计算机中的数据信息的安全。用户需要通过使用账户审计工具,了解系统账户的安全性,掌握安全口令的设置原则,保护系统账户密码的安全,掌握系统账户的管理方法。

7.2 预 备 知 识

7.2.1 Windows Server 2003 的安全标识符

1. Windows Server 2003 的安全特性

(1) IIS 6.0 的安全性:加密服务、摘要认证、过程访问控制等;

(2) Internet 连接防火墙(ICF):软件防火墙,提供端口安全;

(3) 软件限制策略:限制系统运行未授权的可执行程序;

(4) 新的摘要安全包:支持摘要认证协议;

(5) 改善了以太局域网和无线局域网的安全性:促进安全认证和授权;

(6) 凭证管理器:提供了一个口令密码和 X.509 证书的仓库;

(7) 内核模式加密算法:支持 SHA-1、DES、3DES 和随机数发生器;

(8) 改进的 SSL 客户端认证:使会话速度提高 35%;

(9) 增强的 EFS 加密文件系统:提供给多个用户访问多组加密文件的可能。

2. Windows Server 2003 的安全模型

Windows Server 2003 主要包含 6 个主要的安全元素:审计、管理、加密、访问控制、用户验证和安全策略。安全模型的主要功能是用户身份验证和访问控制。

Windows Server 2003 身份验证启用对所有网络资源的单一登录。单一登录允许用户使用一个密码或智能卡一次登录到域,然后向域中任何计算机验证身份。身份验证有交互式登录和网络身份验证两种类型。交互式登录向域账户或本地计算机确认用户身份,域账户存储在 Active Directory 目录服务中,本地计算机账户存储在安全账户管理器(SAM)中。网络身份验证支持包括 Kerberos V5、安全套接字层/传输层安全性(SSL/TLS)以及 NTLM。系统通过用户身份验证控制对网上资源或对象的访问,通过管理对象的属性设置权限、分配所有权以及监视用户访问。

3. Windows Server 2003 的安全认证子系统

本地安全认证子系统(LSASS)接收用户登录凭证,主要包含 5 个关键组件:安全标识符、访问令牌、安全描述符、访问控制列表和访问控制项。

安全标识符(Security Identifiers)即 SID,当创建一个用户或一个组的时候,系统会分配给该用户或组一个唯一 SID。SID 由计算机名、当前时间、当前用户态线程的 CPU 耗费时间的总和 3 个参数决定,以保证它的唯一性。SID 号用空格分隔,或用“-”分隔,例如 S-1-5-21-1763234323-3212657521-1234321321-500。

用户通过验证后,登录进程会给用户一个访问令牌。若改变用户的权限,需要注销后重新登录,重新获取访问令牌。当用户试图访问系统资源时,将访问令牌提供给系统,系统检查用户试图访问对象上的访问控制列表。若用户被允许访问该对象,则系统分配给用户适当的访问权限。

Windows 中的任何对象的属性都有安全描述符这部分,它保存对象的安全配置。

访问控制列表有任意访问控制列表和系统访问控制列表两种。任意访问控制列表包含了用户和组的列表,以及相应的权限:允许或拒绝。每一个用户或组在任意访问控制列表中都有特殊的权限。系统访问控制列表为审核服务,包含了对象被访问的时间。

访问控制项(Access Control Entries)包含了用户或组的 SID 以及对象的权限。它有允许访问和拒绝访问两种,并且拒绝访问的级别高于允许访问。

4. Windows Server 2003 的安全标识符

Windows Server 2003 安全认证子系统中的一个重要组件就是安全标识符(SID),每当系统创建一个用户或一个组的时候,系统就会分配给该用户或组一个唯一的 SID。一旦账号被删除,安全标识符同时被删除。Windows Server 2003 对登录的用户指派权限时,表面上是对账户,实际是根据 SID 号进行。安全标识(SID)是唯一的,即使是相同的用户名,在每次创建时获得的安全标识都完全不同;即使用相同的用户名重建账号,也会被赋予不同的安全标识,不会保留原来的权限。

一个完整的 SID 号包括 SID 的版本号、SID 的颁发机构代码、SID 的子颁发机构代码,以及由计算机名、当前时间、当前用户态线程的 CPU 耗费时间决定的 30 位数字和相对标识符(RID),如图 7-1 所示。



图 7-1 SID(安全标识符)结构

相对标识符(Relative Identifiers,RID)标志域内的账户和组。RID 为 500 的 SID 是系统内置 administrator 账户,即使重命名,其 RID 保持为 500 不变。RID 为 501 的 SID 是 Guest 账户,从 1000 开始的 RID 代表用户账户。例如,RID 为 1005 是该域创建的第 5 个用户。

7.2.2　Windows Server 2003 的安全账户管理器

Windows Server 2003 中对用户账户的安全管理使用了安全账户管理器(Security Account Manager,SAM)的机制。安全账户管理器对账户的管理是通过安全标识进行的。安全账户管理器的具体表现就是%SystemRoot%\system32\config\sam 文件。SAM 文件是系统的用户账户数据库,所有用户的登录名及口令等相关信息都会保存在这个文件中。

SAM 文件的 Hash 加密包括 LanManager(LM)口令散列算法和 NTLM 口令散列算法两种方式。LM 对口令的处理方法是:如果口令不足 14 位,用 0 补足 14 位,并把所有的字母转成大写字母;再将处理后的口令分成两组数字,每组 7 位。由于口令已经被分解为两个 7 个字符长度口令的破解,并且不用测试小写字母,因此破解难度并不高。

因此,微软在 Windows NT4 的 SP3 之后的补丁中提供了一个 syskey. exe 的小工具来进一步加强 NT 的口令。这个软件是可以选择使用的,管理员只要运行该程序并回答一些设置问题就可以添加这项增强功能。

7.2.3　L0phtCrack5 程序

L0phtCrack5(简称 LC5)是著名的美国计算机安全公司组织开发的 Windows 平台口令审核程序,提供了审核 Windows 账户的功能,以提高系统的安全性。LC5 通过破解 SAM 文件来获得用户名和密码。LC5 可以在本地系统、远程系统、系统备份中获得 SAM 文件,从而破解出口令。

LC5 的 4 种破解模式包括字典攻击(Dictionary Attack)、混合攻击(Hybrid Attack)、预设攻击(Precomputed Attack)和暴力攻击(Brute Force Attack)。

7.2.4　账户安全策略

1. 安全密码的设置原则

一般来说,安全密码的口令不应少于 8 个字符,不包含完整的字典词汇,不包含用户名、真实姓名、生日或公司名称等,同时包含大写字母、小写字母、数字、特殊符号 4 类中的 3 类字符。

2. 账户策略

(1) 密码长度最小值:8 个字符;

(2) 密码最长存留期:42 天;

(3) 密码最短存留期:1 天;

(4) 强制密码历史:24 个。

7.3 方案设计

方案设计如表 7-1 所示。

表 7-1 方案设计

任务名称	系统的账户管理
任务分解	1. 安全标识符的查看 (1) 使用 user2sid 工具软件查看某账户的 SID (2) 手动查看某账户的 SID (3) 使用 sid2user 工具软件，已知 SID，查看其用户名 2. SYSKEY 双重加密账户保护 3. 使用 LC5 审计账户的安全性 (1) 利用向导进行本地审计 (2) 利用进程进行本地审计 (3) 利用进程进行远程审计 (4) 利用 SAM 文件进行审计 4. 账户的安全防护 (1) 利用注册表进行安全防护 (2) 利用本地安全设置进行安全防护 (3) 利用账户安全策略进行安全防护
能力目标	1. 能使用 user2sid 工具软件查看账户的安全标识符 2. 能手动查看账户的安全标识符 3. 能使用 sid2user 工具软件由安全标识符查看账户名 4. 能使用 SYSKEY 双重加密系统账户 5. 能使用口令审核程序 LC5 利用向导审计本地系统账户安全性 6. 能使用口令审核程序 LC5 利用进程审计本地系统账户安全性 7. 能使用口令审核程序 LC5 利用进程审计远程账户安全性 8. 能使用口令审核程序 LC5 利用 SAM 文件进行审计 9. 能使用注册表进行系统的安全防护 10. 能利用本地安全设置进行安全防护 11. 能利用账户安全策略进行安全防护
知识目标	1. 了解 Windows Server 2003 的安全特性 2. 了解 Windows Server 2003 的安全认证过程 3. 掌握 Windows Server 2003 账户的管理 4. 熟悉 Windows Server 2003 安全账户的安全防护 5. 掌握 Windows Server 2003 账户审计工作的原理与使用 6. 了解 Windows Server 2003 注册表原理与结构
素质目标	1. 树立较强的安全意识 2. 培养良好的职业道德 3. 掌握网络安全行业的基本情况 4. 树立较强的安全、节约、环保意识 5. 培养职业兴趣，以及爱岗敬业、热情主动的工作态度

7.4　任务实施

为了完成本工作任务，划分以下4个子任务。

7.4.1　任务1：安全标识符的查看

1. 任务目标

通过第三方工具的使用或手动操作，查看本地或远程系统的安全标识符，从而判断账户是否为administrator账户。

2. 工作任务

(1) 使用user2sid工具软件查看某账户的SID；

(2) 手动查看某账户的SID；

(3) 使用sid2user工具软件，已知SID，查看其用户名。

3. 工作环境

(1) 两台预装Windows Server 2003/XP的主机，通过网络相连。

(2) 软件工具：user2sid、sid2user。

4. 实施过程

(1) 使用user2sid工具软件查看某账户的SID

在Windows Server 2003/XP系统中利用user2sid命令查看某账户SID的具体步骤如下：

① 选择"开始"→"运行"菜单项，打开"运行"对话框。在"打开"下拉列表文本框中输入"cmd"，然后单击"确定"按钮。

② 在"命令提示符"窗口中输入命令，转到user2sid命令所在目录，如图7-2所示。

```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>cd sid

C:\sid>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 88A1-9CD1

 C:\sid 的目录

2010-11-14  15:51    <DIR>          .
2010-11-14  15:51    <DIR>          ..
1998-04-26  21:21            49,152 sid2user.exe
1998-04-26  21:21            49,152 user2sid.exe
1998-04-26  21:24             1,238 welcome.html
               3 个文件         99,542 字节
               2 个目录  1,716,097,024 可用字节

C:\sid>
```

图7-2　在"命令提示符"窗口中找到user2sid命令

③ 查看本地账户 SID 的命令格式为“user2sid＋空格＋账户”，这里查看管理员账户的 SID 号，即在“命令提示符”窗口输入“user2sid administrator”，然后按下“Enter”键，如图 7-3 所示。

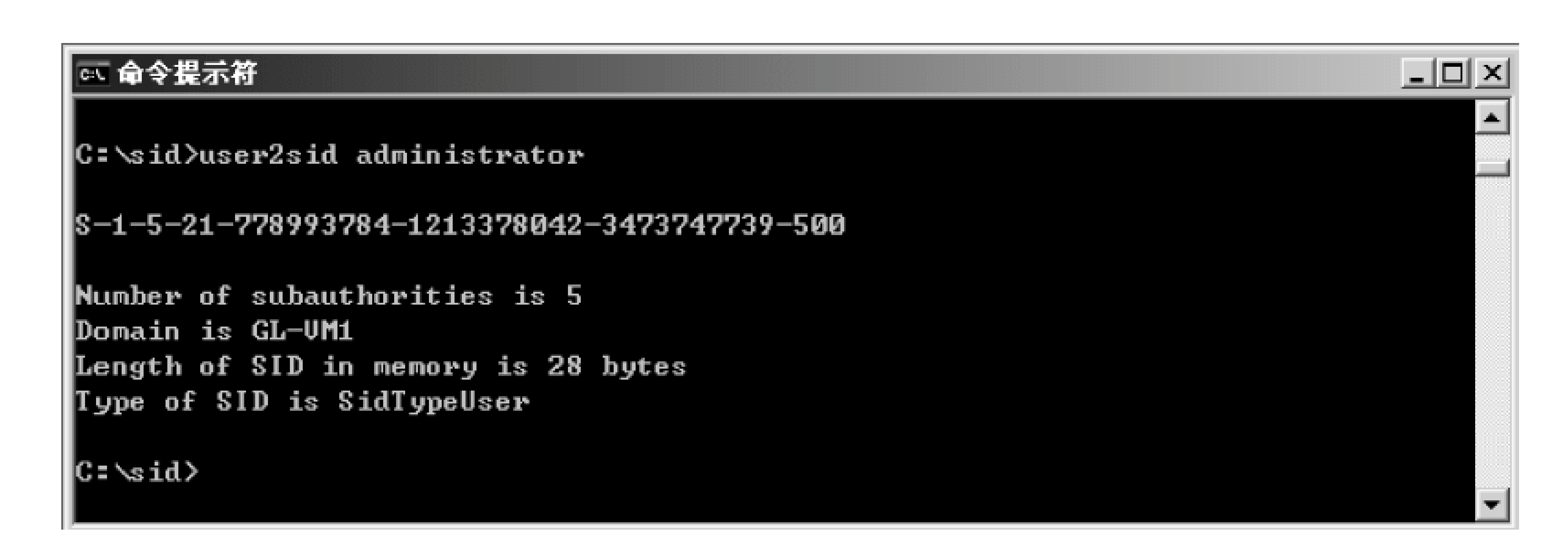


图 7-3 在“命令提示符”窗口查看管理员账户的 SID 号

④ 在“命令提示符”窗口输入“user2sid guest”，然后按下“Enter”键，可以查看 guest 账户的 SID 号，如图 7-4 所示。

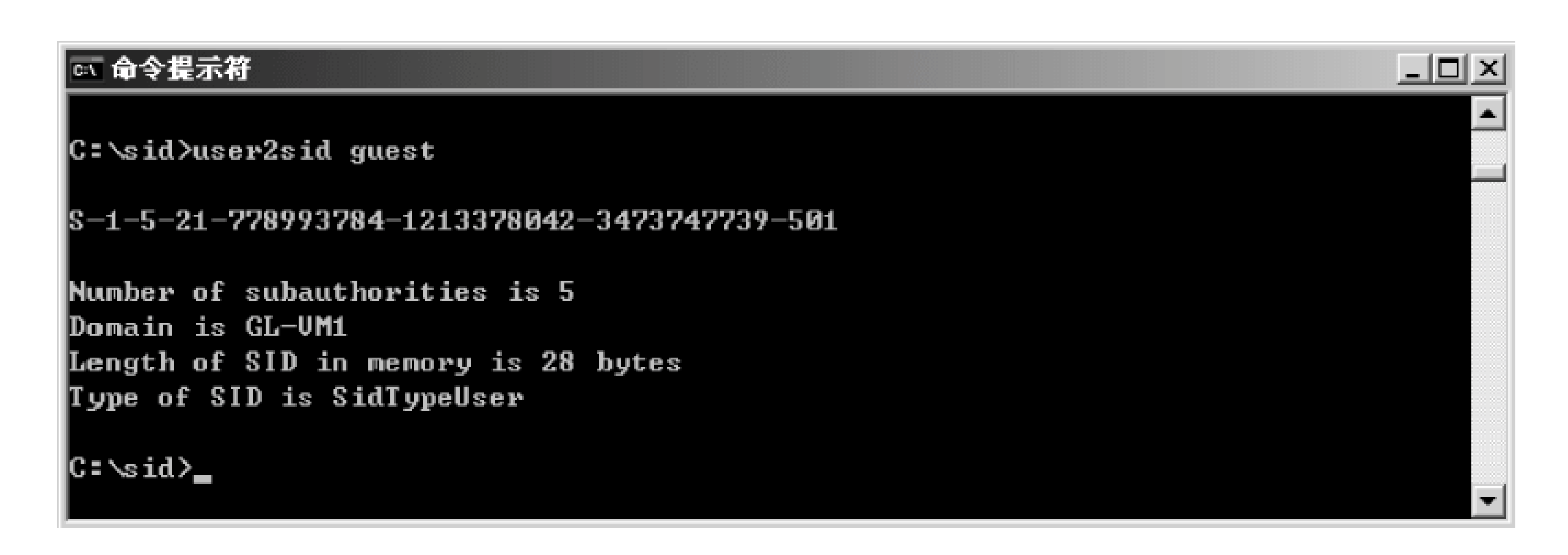


图 7-4 在“命令提示符”窗口查看 guest 账户的 SID 号

⑤ 查看远程主机账户 SID 的命令格式为“user2sid＋空格＋\\IP 地址＋空格＋"账户"”。这里查看远程主机账户“bob”的 SID，远程主机的 IP 地址是 222.19.221.75，即在命令提示符窗口输入“user2sid \\222.19.221.75 "bob"”，然后按下“Enter”键，如图 7-5 所示。

```
D:\Program Files\sid>user2sid \\222.19.221.75 "bob"

S-1-5-21-57989841-2025429265-1801674531-1003

Number of subauthorities is 5
Domain is HOME-0BC72E4B03
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

D:\Program Files\sid>_
```

图 7-5 在“命令提示符”窗口查看远程主机账户的 SID 号

(2) 手动查看某账户的 SID

如果没有 user2sid 工具，或者系统不允许安装第三方软件，则需要手动操作来查看某账户的 SID。方法是首先建立一个账户，并制定该账户对某个文件夹的访问权限；其次删除该账户，注销系统后重新登录，查看该文件的权限设置，就可以看到删除账户的 SID。具体操作步骤如下：

① 右击“我的电脑”，然后选择“管理”菜单，在“计算机管理”→“系统工具”→“本地用户和组”→“用户”空白处右击，如图 7-6 所示。



图 7-6 “计算机管理”窗口

② 选择“新用户”，创建新用户 test，如图 7-7 所示。

③ 右击共享文件夹“gl”的“属性”菜单，弹出“gl 属性”对话框，然后选择“共享该文件夹”，如图 7-8 所示。



图 7-7 “新用户”对话框

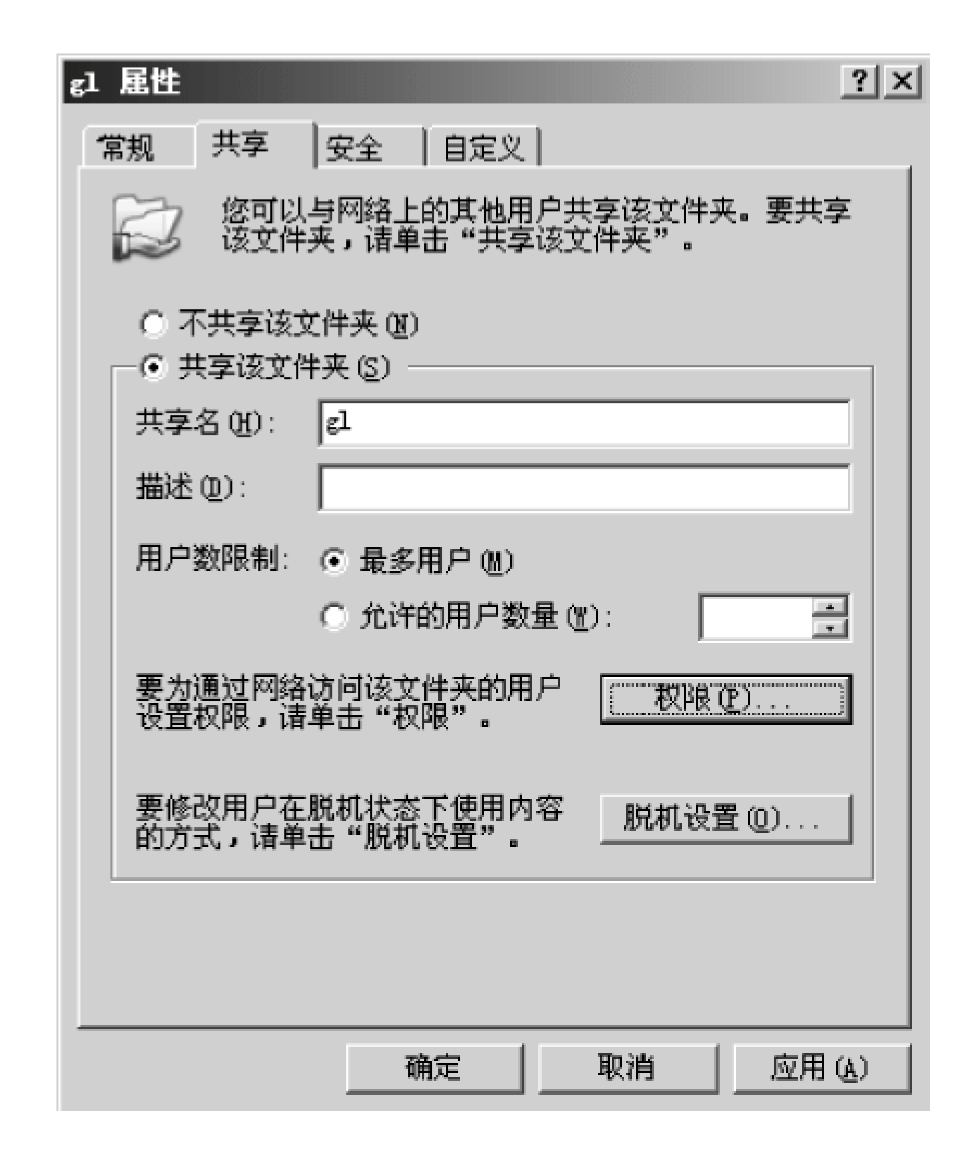


图 7-8 “gl 属性”对话框

④ 单击“权限”按钮，弹出“gl 的权限”对话框，如图 7-9 所示。

⑤ 单击“添加”按钮，在“选择用户或组”对话框中输入账户“test”，然后单击“确定”按钮，如图 7-10 所示。



图 7-9 “gl 的权限”对话框

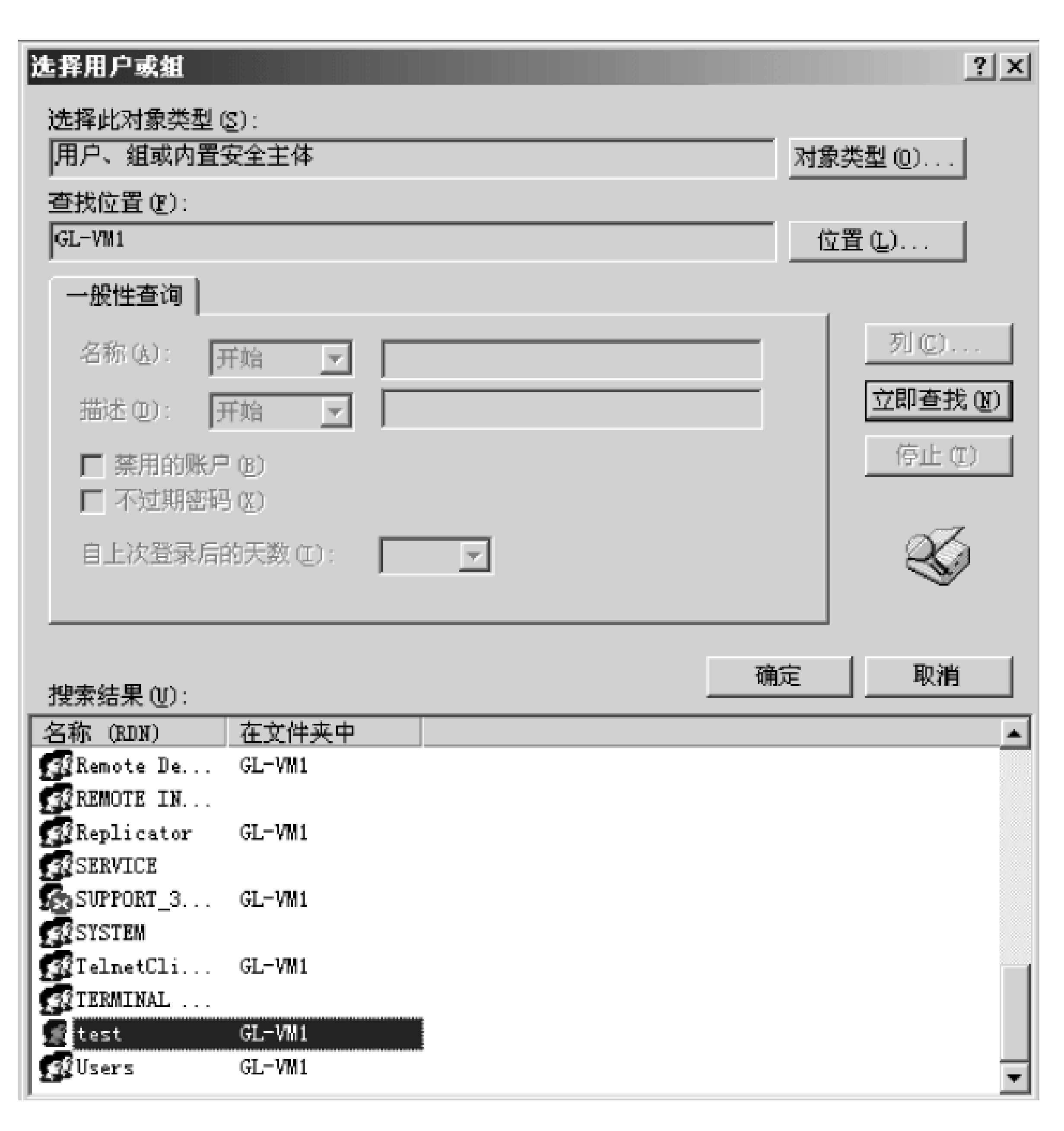


图 7-10 “选择用户或组”对话框

⑥ 在“gl 的权限”对话框中，勾选 test 的权限为允许“读取”，然后单击“确定”按钮，如图 7-11 所示。

⑦ 在“计算机管理”窗口中，删除本地用户“test”。

⑧ 注销并用原来的登录账户重新登录。

⑨ 右击共享文件夹“gl”的“属性”菜单，弹出“gl 属性”对话框。选择“共享该文件夹”，然后单击“权限”按钮，弹出“gl 的权限”对话框，就可以看到刚才创建的 test 账户的 SID，如图 7-12 所示。



图 7-11 设置 test 的权限



图 7-12 查看账户 test 的 SID

(3) 使用 sid2user 工具软件，已知 SID，查看其用户名

在 Windows Server 2003/XP 系统中利用 sid2user 工具软件可以通过 SID 号查看用户

名。黑客在入侵时，可以通过这样的方法获得账户名并判断是否为 administrator 账户。具体操作步骤如下：

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“cmd”，然后单击“确定”按钮。

② 在命令行提示符窗口中输入命令，转到 sie2user 命令所在目录。

③ 利用 SID 查看本地账户的命令格式为“sid2user＋空格＋SID 号”。这里通过 SID 号 5-21-778993784-1213378042-3473747739-500 来查看用户名，即在命令提示符窗口输入“sid2user 5-21-778993784-1213378042-3473747739-500”，然后按下“Enter”键，如图 7-13 所示。

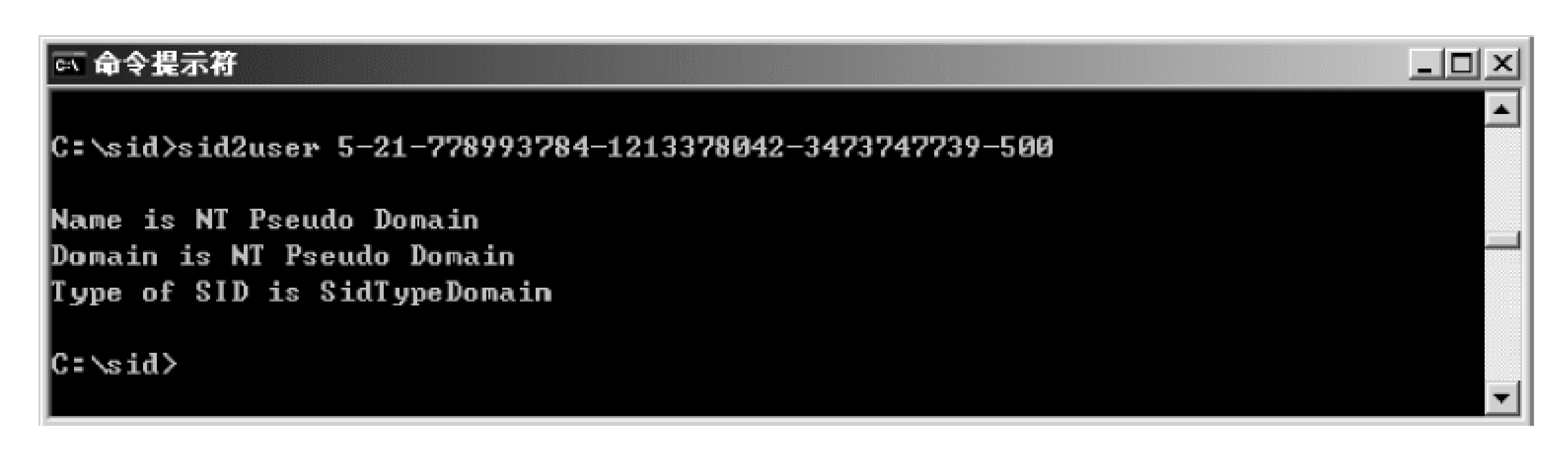


图 7-13　在“命令提示符”窗口利用 SID 号查看账户

④ 利用 SID 查看远程主机账户的命令格式为“sid2user＋空格＋\\IP 地址＋空格＋SID 号”。这里通过 SID 号 5 21 57989841 2025429265 1801674531 1003 来查看用户名，即在命令提示符窗口输入“sid2user \\222.19.221.75 5 21 57989841 2025429265 1801674531 1003”，然后按下“Enter”键，如图 7-14 所示。

```
D:\Program Files\sid>sid2user \\222.19.221.75 5 21 57989841 2025429265 180167453
1 1003

Name is bob
Domain is HOME-0BC72E4B03
Type of SID is SidTypeUser

D:\Program Files\sid>
```

图 7-14　在“命令提示符”窗口利用 SID 号查看远程主机账户

7.4.2　任务 2：SYSKEY 双重加密账户保护

1. 任务目标

通过系统自带的小工具 SYSKEY 对系统的安全账户管理器 SAM 进行二次加密。

2. 工作任务

使用 SYSKEY 双重加密账户保护。

3. 工作环境

两台预装 Windows Server 2003/XP 的主机，通过网络相连。

4. 实施过程

在 Windows Server 2003/XP 系统中通过系统自带的小工具 SYSKEY 对系统的安全账户管理器 SAM 进行二次加密的步骤如下：

(1) 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“syskey.exe”，然后单击“确定”按钮。

(2) 在弹出的"保证 Windows 账户数据库的安全"窗口中,单击"确定"按钮,如图 7-15 所示,完成对 SAM 文件的二次加密。此时没有设置双重启动密码,是系统产生的密码,密码直接保存在注册表中。

(3) 单击"更新"按钮,进入密码设置窗口,如图 7-16 所示。

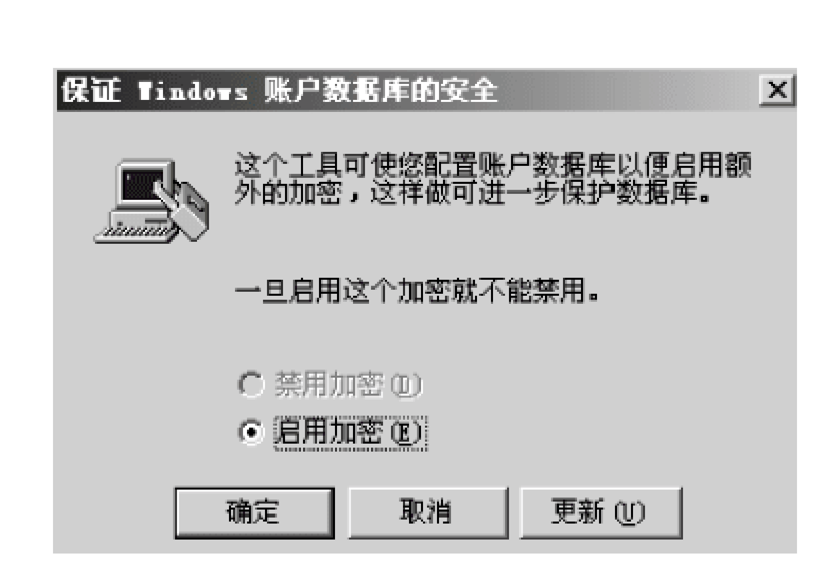


图 7-15 "保证 Windows 账户数据库的安全"窗口

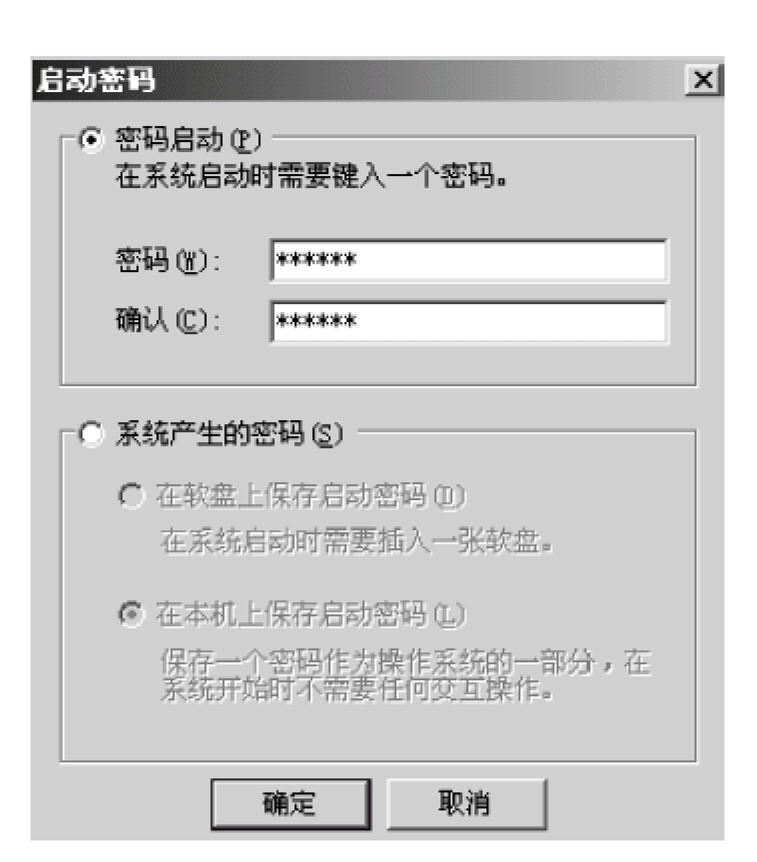


图 7-16 "启动密码"对话框

(4) 选择"密码启动",然后输入密码并确认,再单击"确认"按钮。

(5) 若选择"系统产生的密码",可以选择密码的保存方式。

如果选择"在软盘上保存启动密码",会提示输入所设定的启动密码;插入空白的软盘,确定后密码文件保存在软盘上。设置完成后,下次启动计算机时,会提示插入密码软盘,验证成功后才能进入系统。

如果选择"在本机上保存启动密码",确定后输入刚才设置的启动密码,则启动密码保存到硬盘上,启动时不会显示启动密码的窗口。

7.4.3 任务 3:使用 LC5 审计账户的安全性

1. 任务目标

通过美国计算机安全公司@stake 的口令审核程序审核本地和远程 Windows 账户的安全性。

2. 工作任务

(1) 利用向导进行本地审计;

(2) 利用进程进行本地审计;

(3) 利用进程进行远程审计;

(4) 利用 SAM 文件进行审计。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机,通过网络相连。

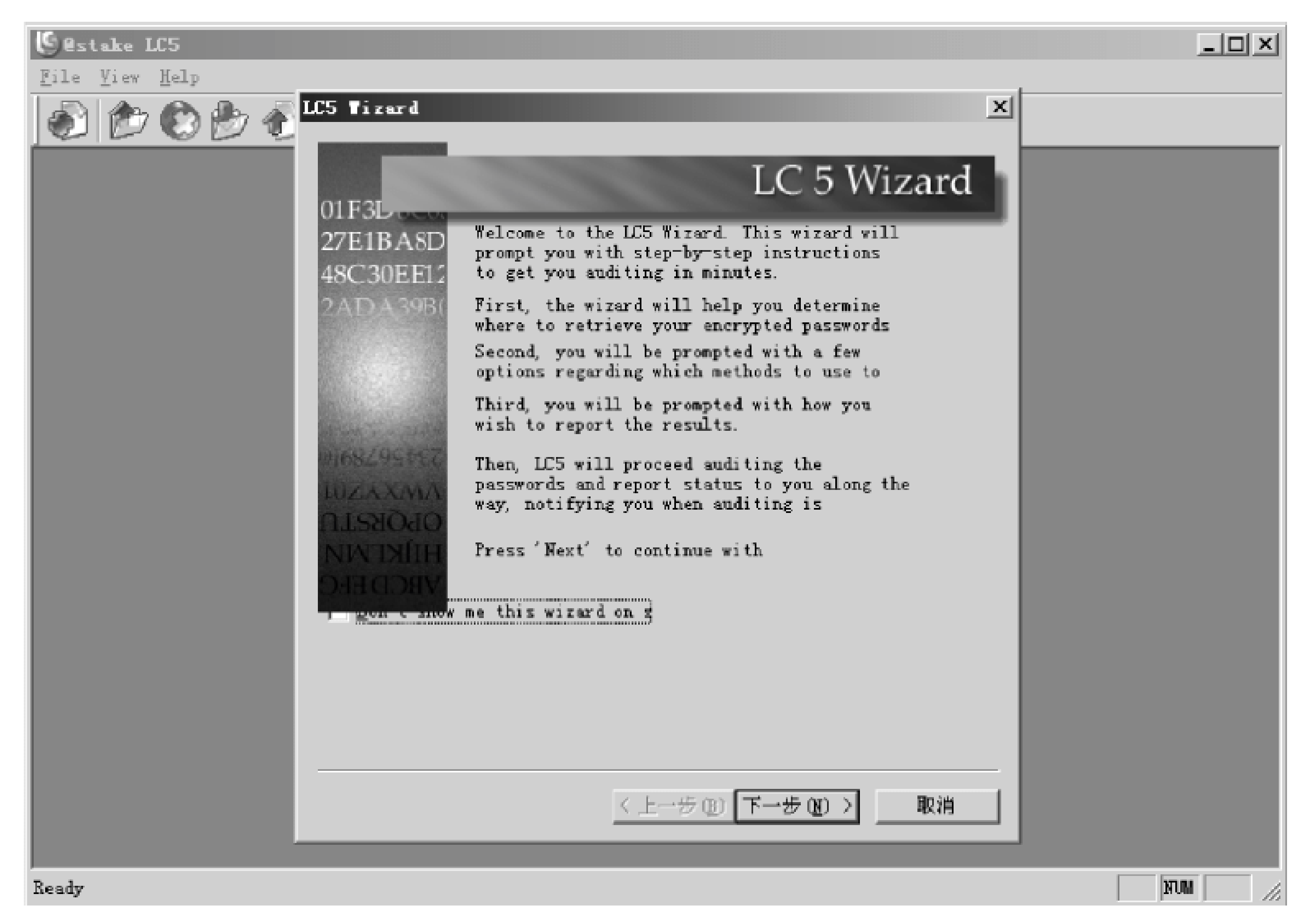
(2) 软件工具:L0phtCrack5。

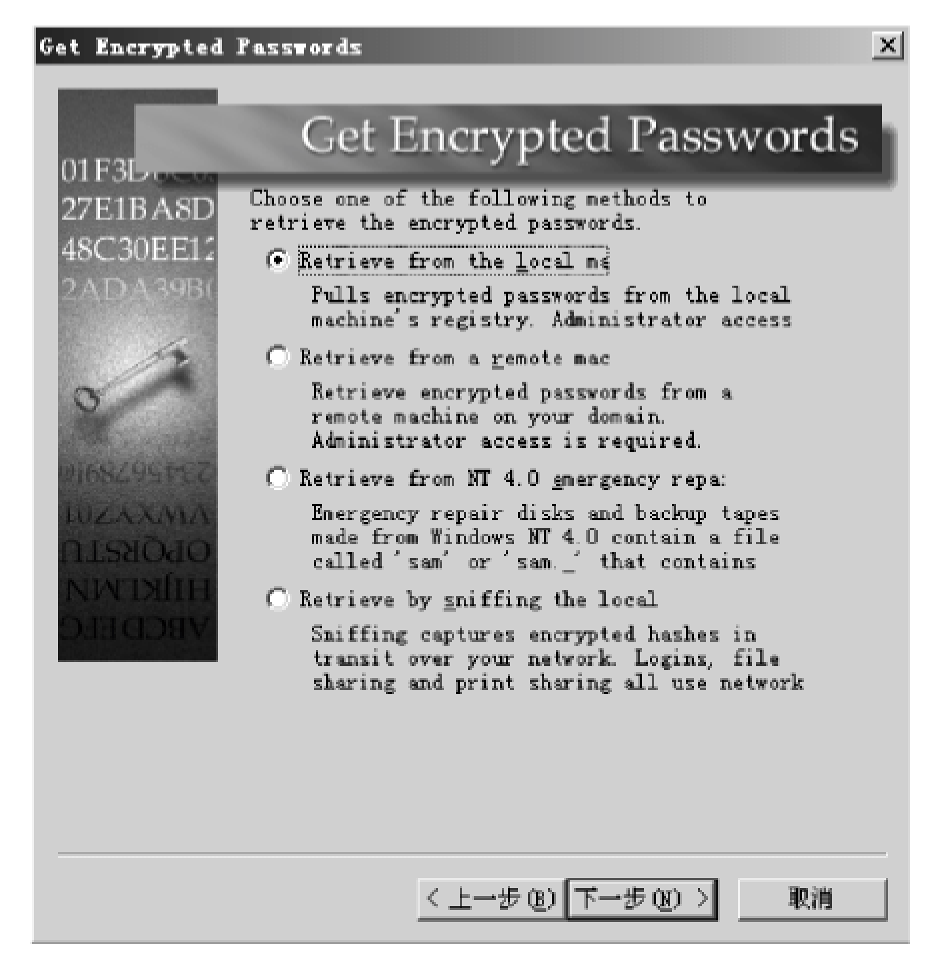
4. 实施过程

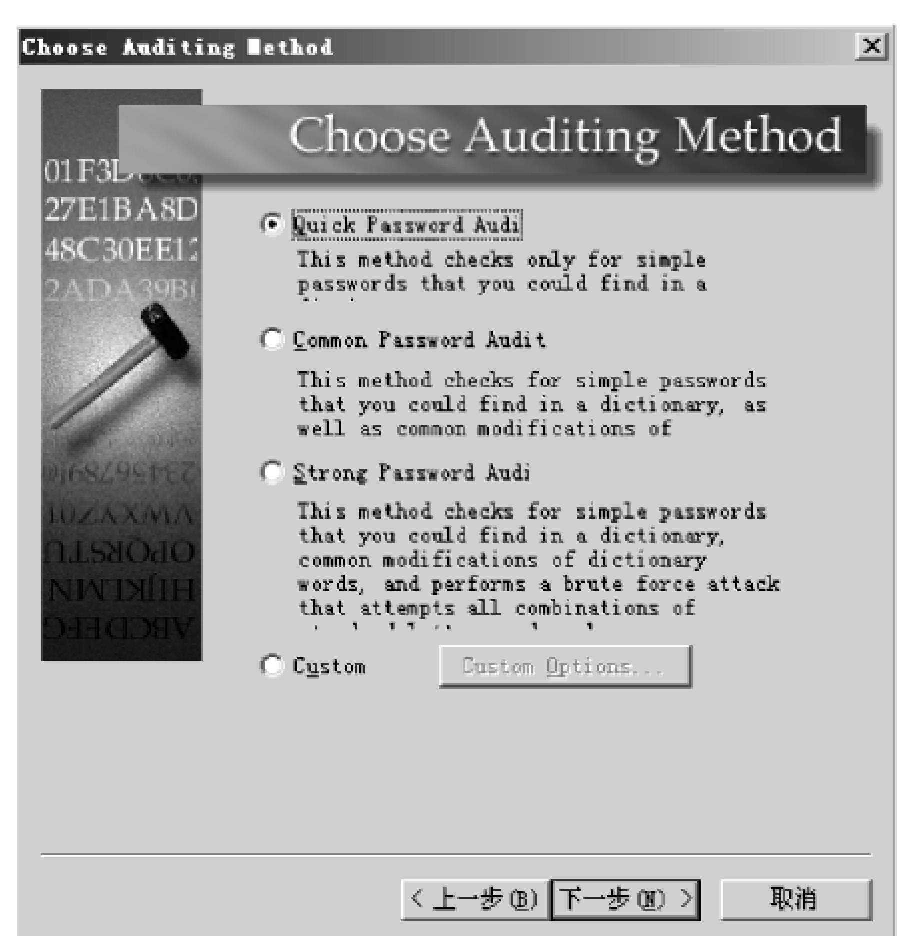
(1) 利用向导进行本地审计

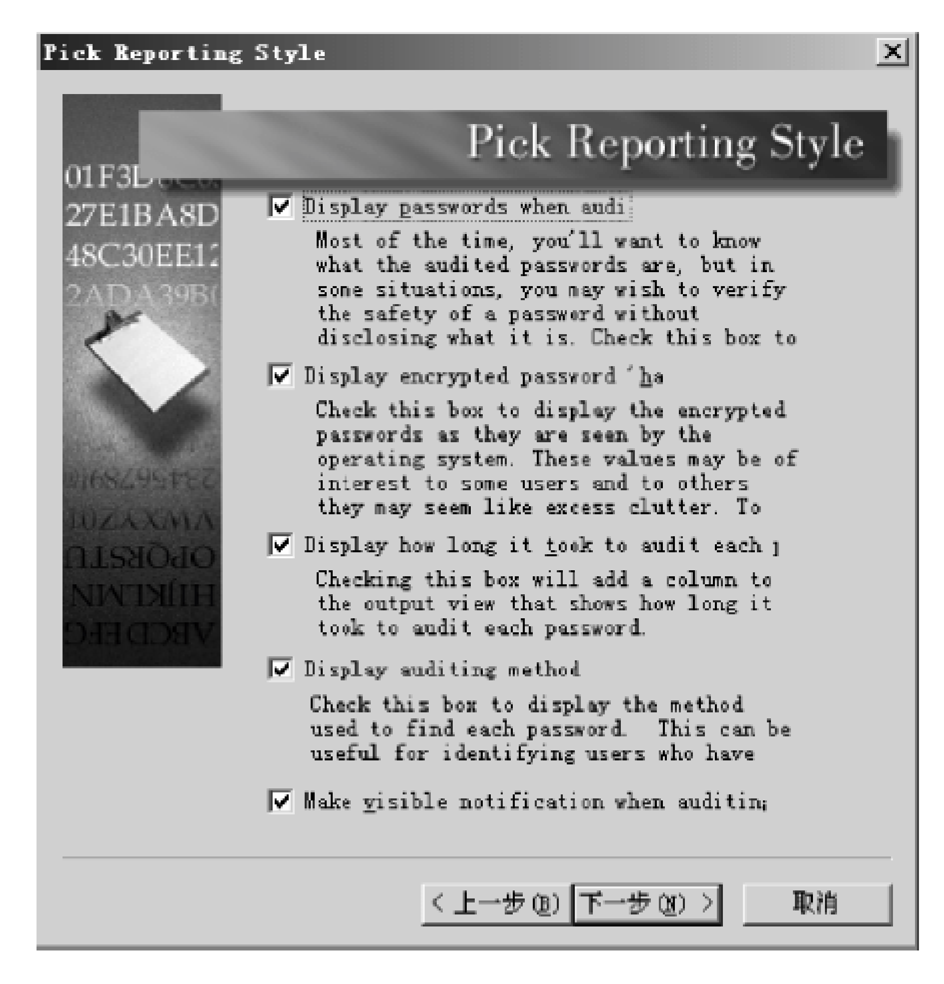
① 首先建立实验账户 a,密码是 123456;实验账户 b,密码是 abcabc;实验账户 c,密码是 123abc;实验账户 d,密码是 abc123;实验账户 e,密码是 12344321;实验账户 f,密码是 abcd1234。

② LC5 的安装很简单。安装完毕后，打开 LC5，默认运行 LC5 向导，如图 7-17 所示。









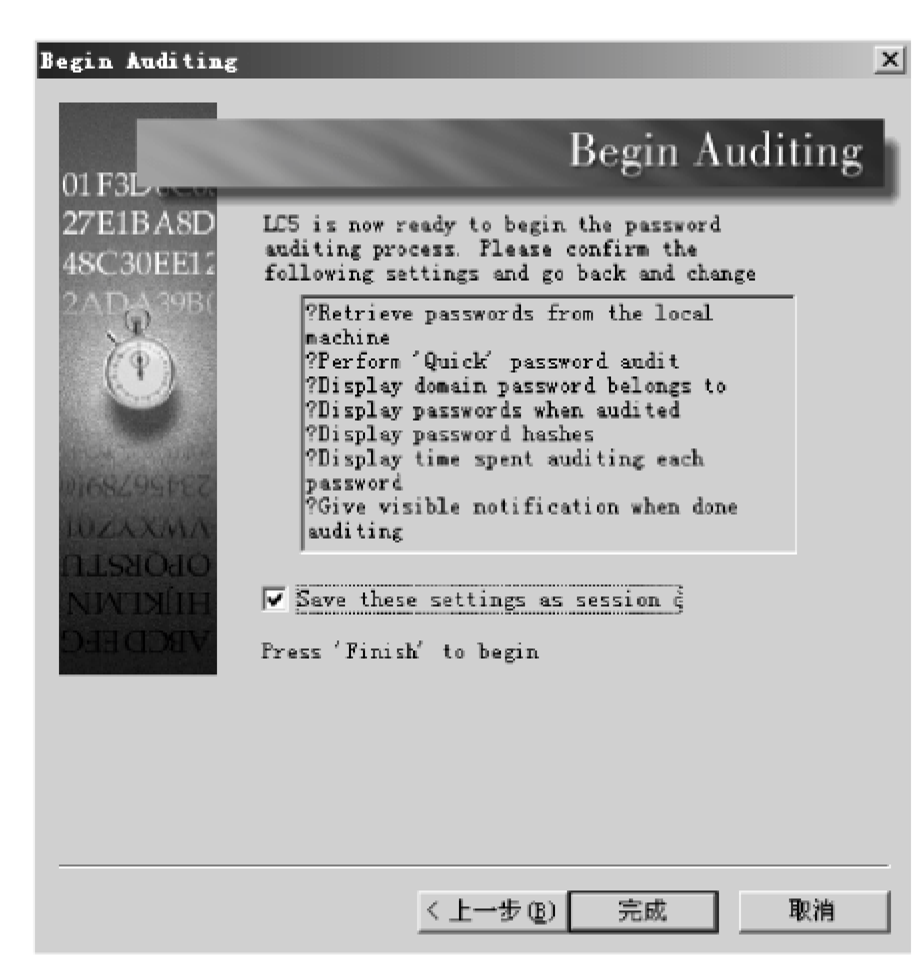


图 7-17　安装向导

③ 向导设置完成之后。会出现本次审计的结果，如图 7-18 所示。

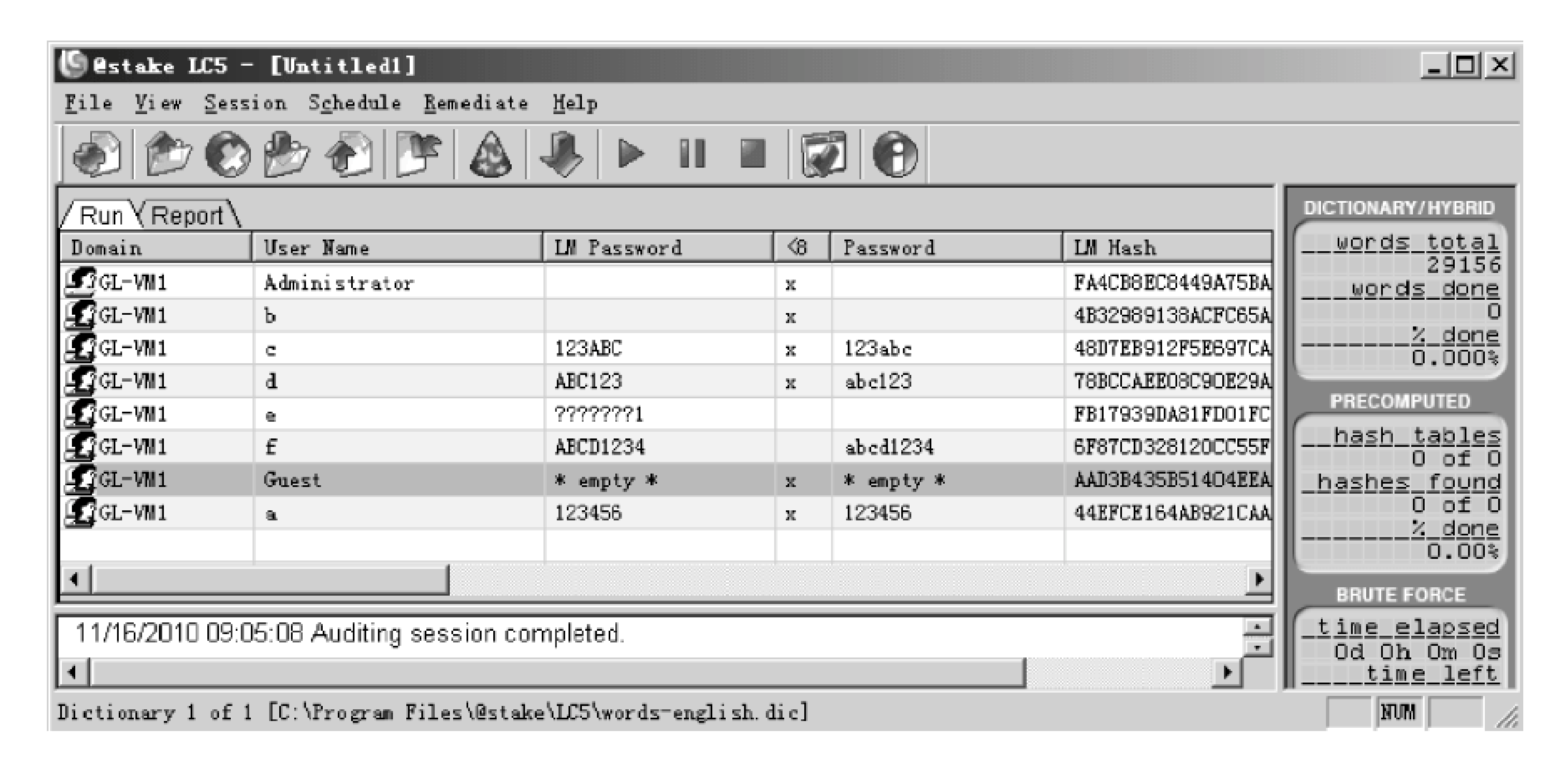


图 7-18 “@stake LC5”窗口中显示的审计结果

（2）利用进程进行本地审计

如果不用向导开始，可以利用进程进行本地账户审计。

① 选择“File”菜单中的“New Session”，新建一个会话。然后，选择“Session”菜单中的“Import”，再在“Import”对话框中选中“Local machine”项，如图 7-19 所示。

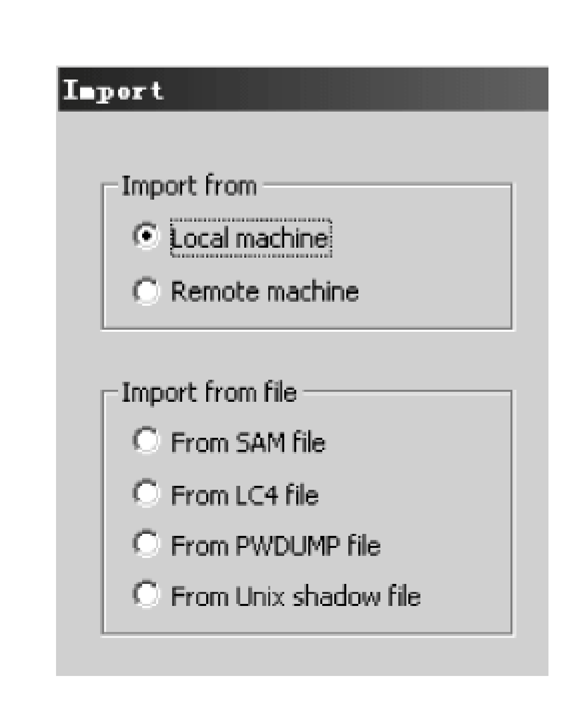


图 7-19 “Import”对话框(1)

② 单击“OK”按钮，弹出“@stake LC5”主窗口界面，如图 7-20 所示，显示出从本地主机中导入的 8 个账户。

③ 选择“Session”菜单中的“Session Option”，对本次破解的模式与破解字典进行设置，如图 7-21 所示。

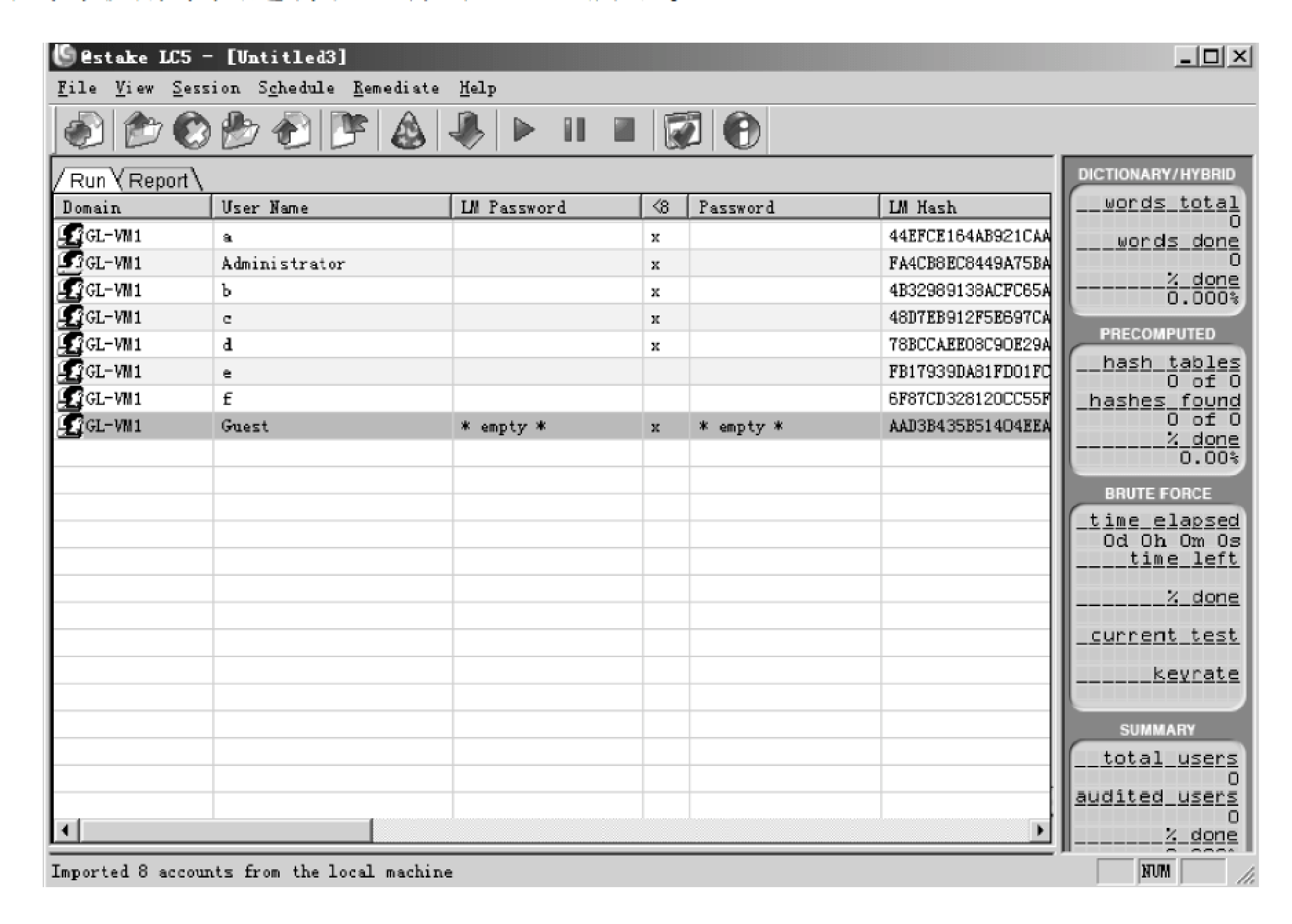


图 7-20 “@stake LC5”窗口中显示导入的 8 个账户

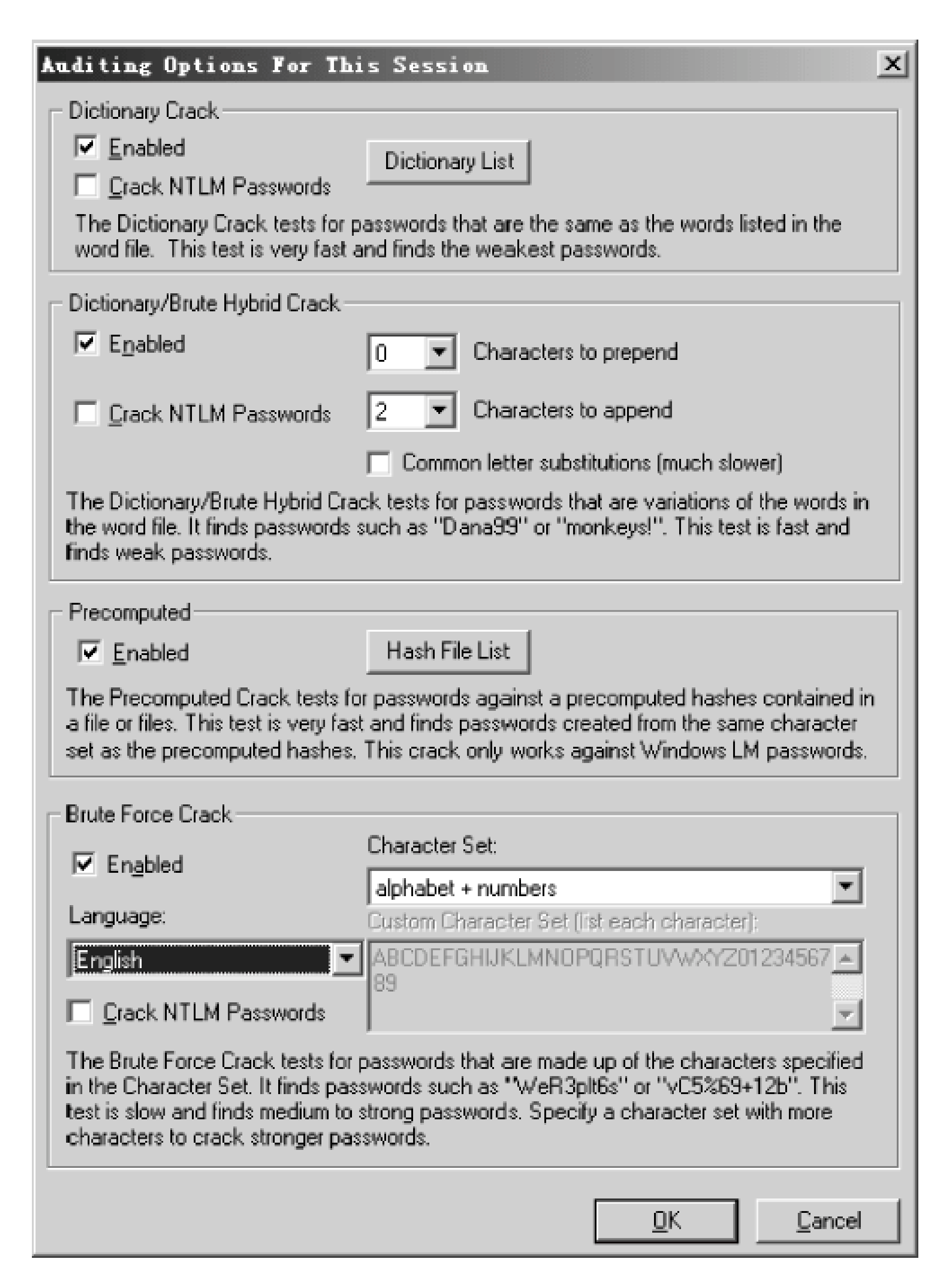


图 7-21　“Auditing Options For This Session”对话框

在“Auditing Options For This Session”对话框中有 4 种破解模式：字典攻击(Dictionary Attack)、混合攻击(Hybrid Attack)、预设攻击(Precomputed Attack)和暴力攻击(Brute Force Attack)。把 4 种破解模式都选上，然后单击“OK”按钮。

④ 单击“Session”菜单中的“Begin Audit”按钮，或按快捷键 F4，或单击工具栏中的“运行”按钮开始破解。

(3) 利用进程进行远程审计

利用进程进行远程审计的步骤如下：

① 选择“File”菜单中的“New Session”，新建一个会话。然后，选择“Session”菜单中的“Import”，再在“Import”对话框中选中“Remote machine”项，如图 7-22 所示。

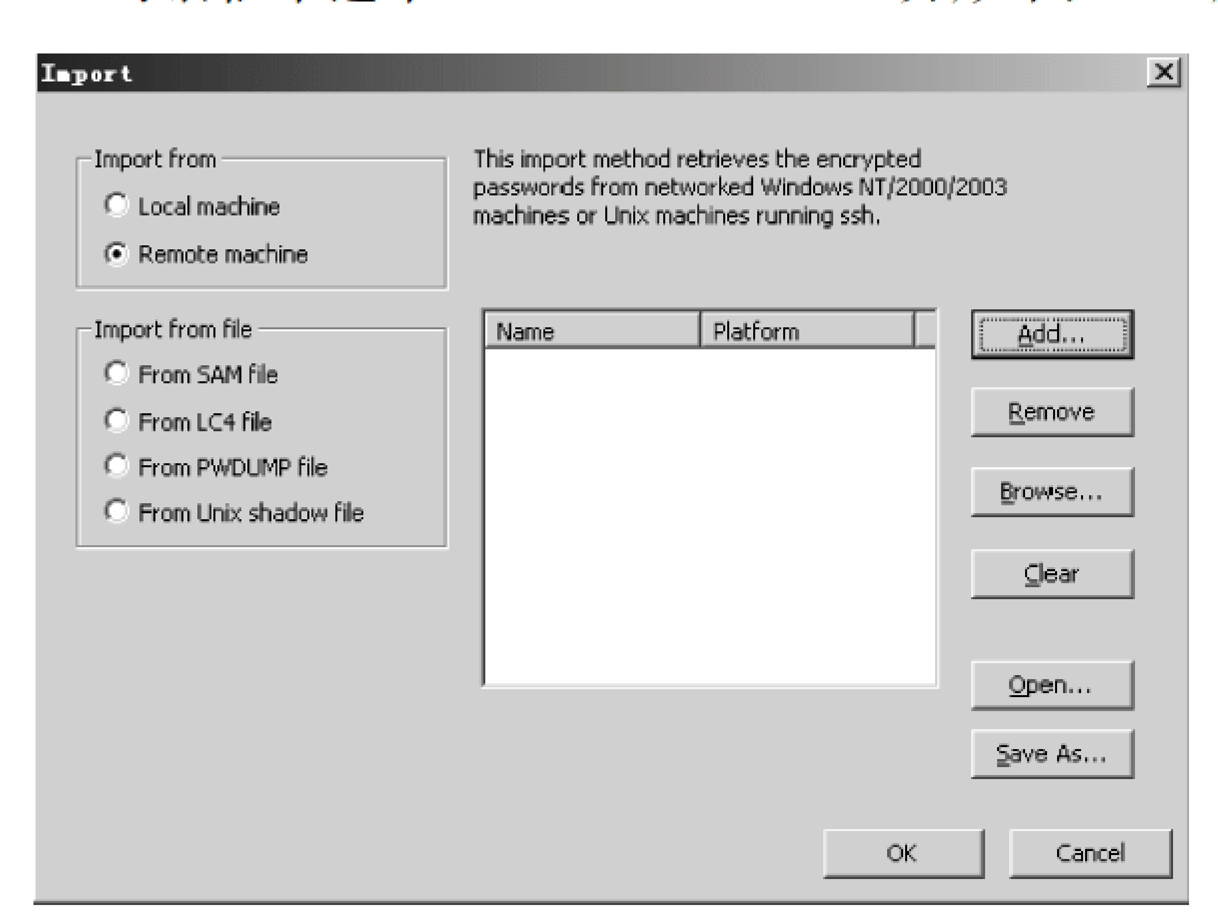


图 7-22　“Import”对话框(2)

② 在“Import”对话框中单击“Add”按钮。

③ 在弹出的“Add Machine to Remote Import”对话框中输入远程主机的 IP 地址，并单击“OK”按钮，如图 7-23 所示。

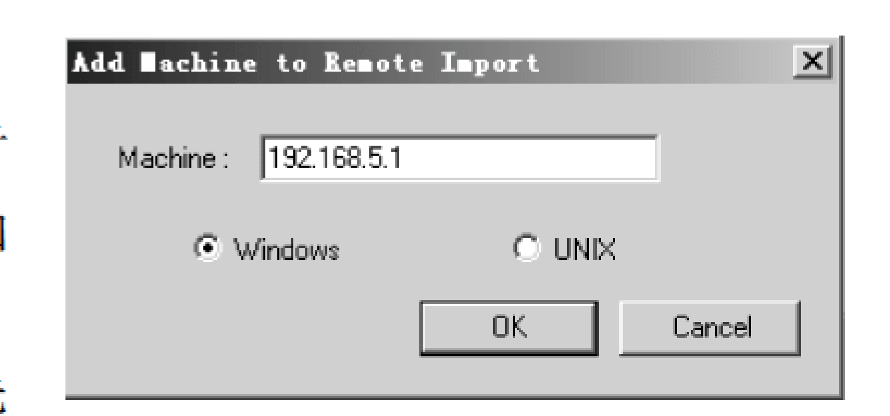


图 7-23 “Add Machine to Remote Import”对话框

④ 在弹出的“Enter Credentials”对话框中输入远程主机中具有管理员权限的账户和密码，并单击“OK”按钮，如图 7-24 所示。

⑤ 在“Import”对话框单击“OK”按钮，会弹出“Warning!”窗口，如图 7-25 所示。单击两次“OK”按钮，即可导入远程会话，然后开始审计，方式与前面类同。

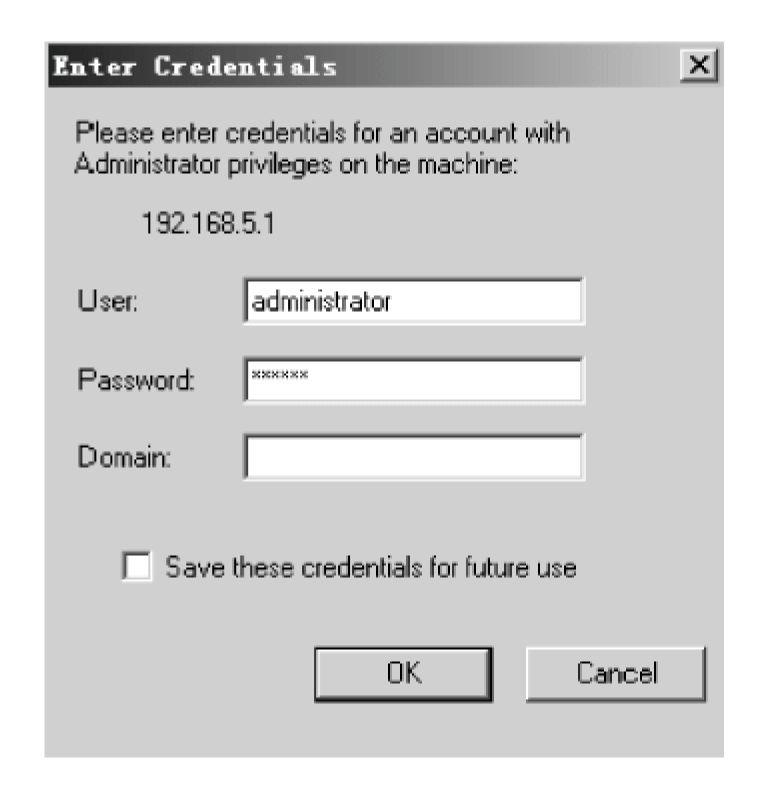


图 7-24 “Enter Credentials”对话框

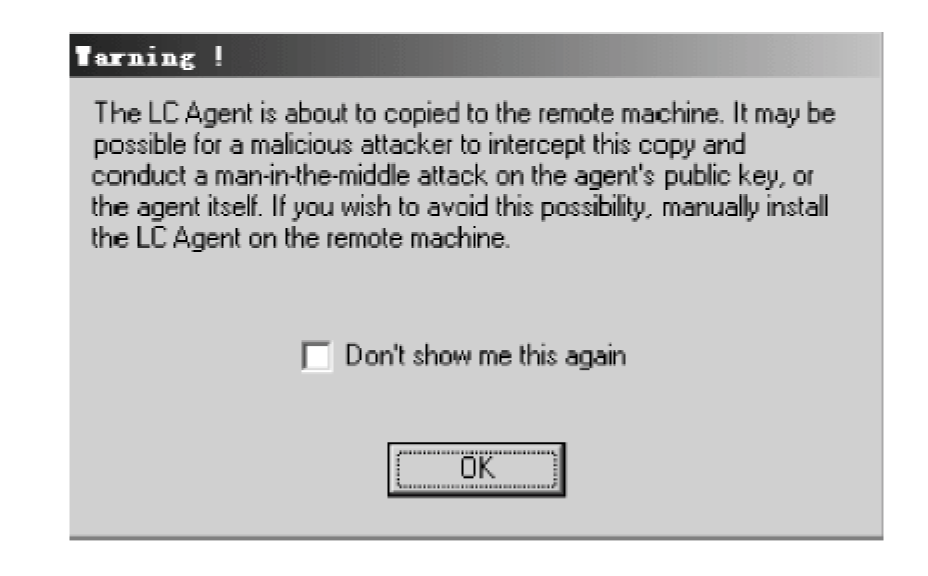


图 7-25 “Warning!”窗口

(4) 利用 SAM 文件进行审计

利用 SAM 文件进行远程审计的步骤如下：

① 用“超级兔子”获得 SAM 文件。

② 选择“File”菜单中的“New Session”，新建一个会话。然后，选择“Session”菜单中的“Import”，再在“Import”对话框中选中“From SAM file”项，如图 7-26 所示。

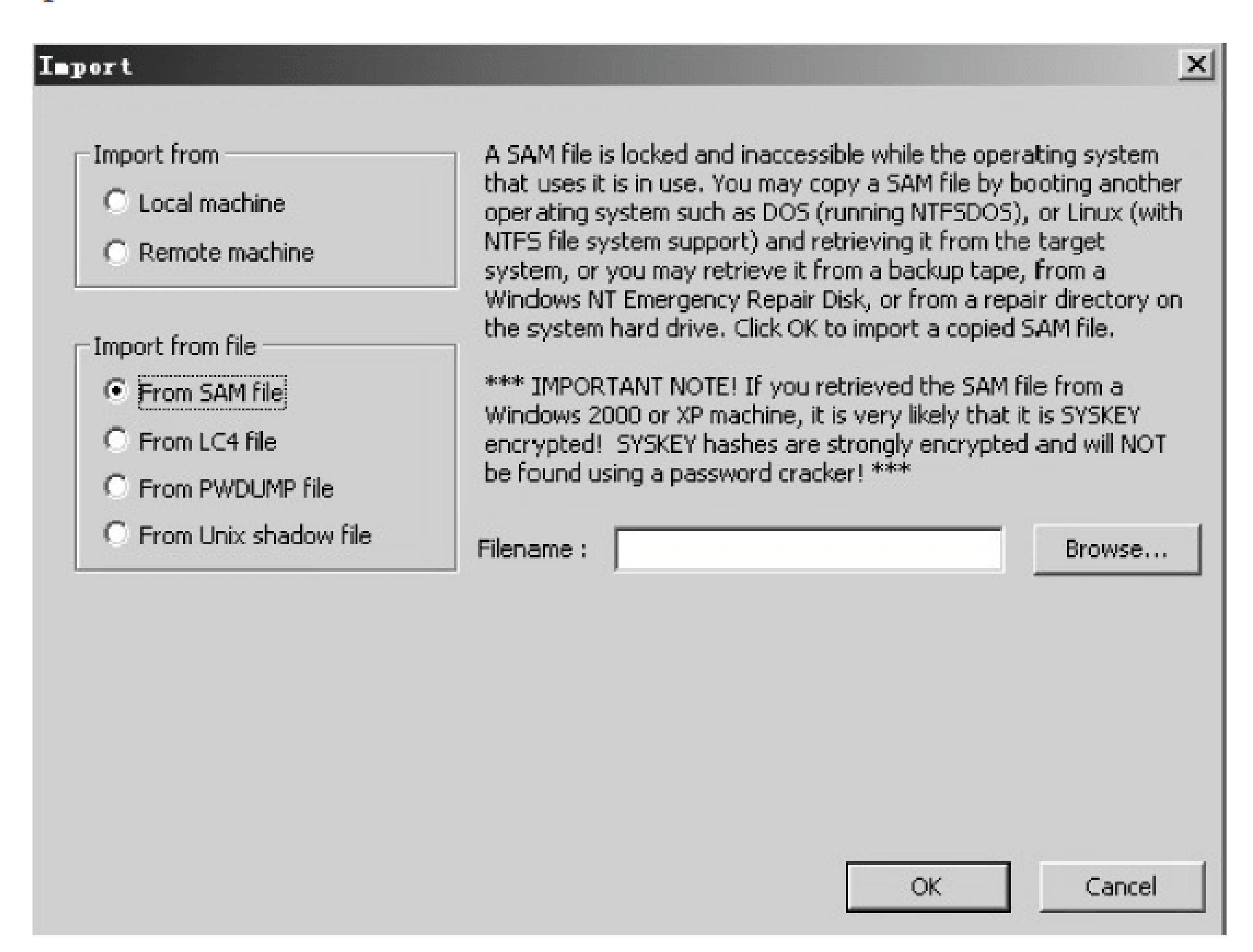


图 7-26 “Import”对话框(3)

7.4.4　任务 4：账户的安全防护

1. 任务目标

通过修改注册表或设置本地安全策略维护 Windows 账户的安全性。

2. 工作任务

（1）利用注册表进行安全防护；

（2）利用本地安全设置进行安全防护；

（3）利用账户安全策略进行安全防护。

3. 工作环境

两台预装 Windows Server 2003/XP 的主机，通过网络相连。

4. 实施过程

（1）利用注册表进行安全防护

如果没有需要 LM 身份验证的客户机，应禁用 LM 散列的存储，从而避免非法入侵者利用 LC5 破解 Windows 用户口令。具体操作步骤如下：

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“regedit”，然后单击“确定”按钮。

② 将注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 的一个子项 nolmhash 的键值改为“1”，如图 7-27 所示。

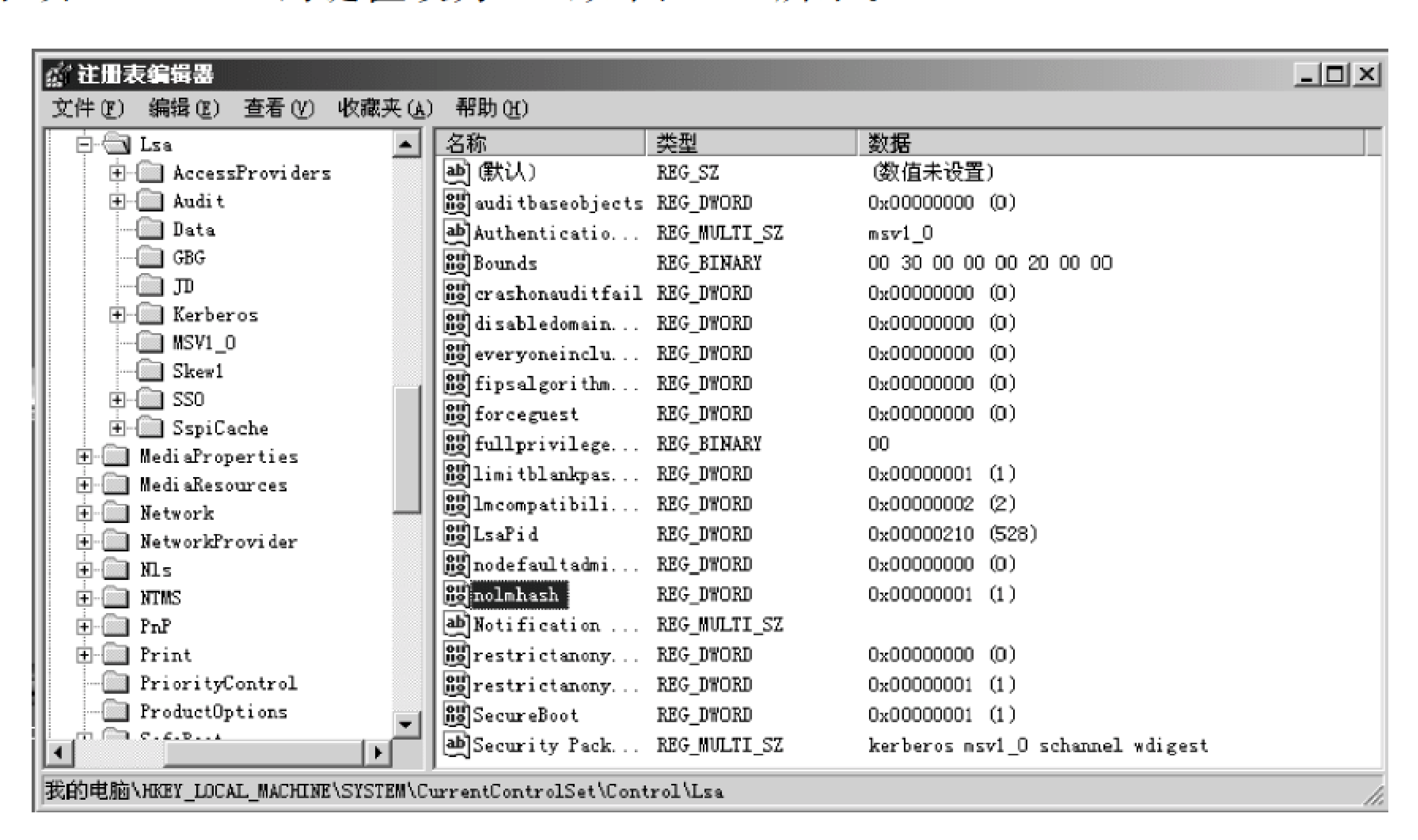


图 7-27　注册表信息

③ 修改完注册表后，重新启动或注销系统。

④ 新建账户，然后导入 LC5 进行审计。

⑤ 从审计的结果可以看到，新建的账户密码没有被破解。由此可见，注册表修改能有效防御针对 LM 散列的攻击。

（2）利用本地安全设置进行安全防护

如果不修改注册表的值，可以利用本地安全策略的设置进行安全防护，具体操作步骤

如下：

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“secpol.msc”，然后单击“确定”按钮，如图 7-28 所示。

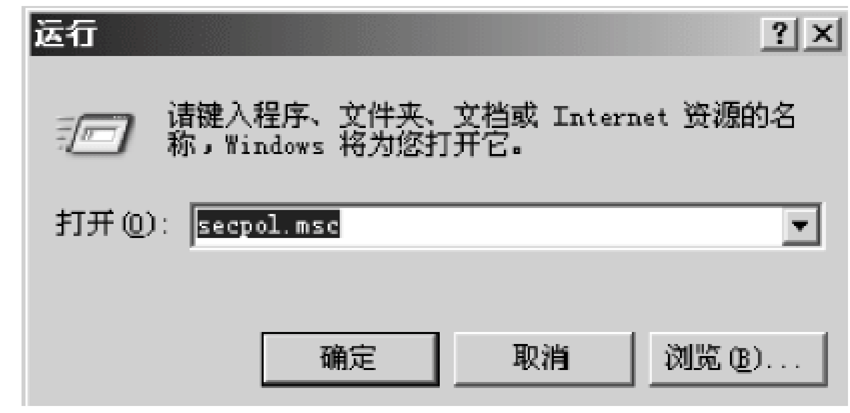


图 7-28 “运行”对话框

② 在本地安全设置中，选择“安全设置”→“本地策略”→“安全选项”菜单项。

③ 在右侧窗口双击“网络安全：不要在下次更改密码时存储 LAN Manager 的哈希值”，在弹出的对话框中选择“已启用”，然后单击“确定”按钮，如图 7-29 所示。这样，就可以阻止针对 LM 散列的攻击。

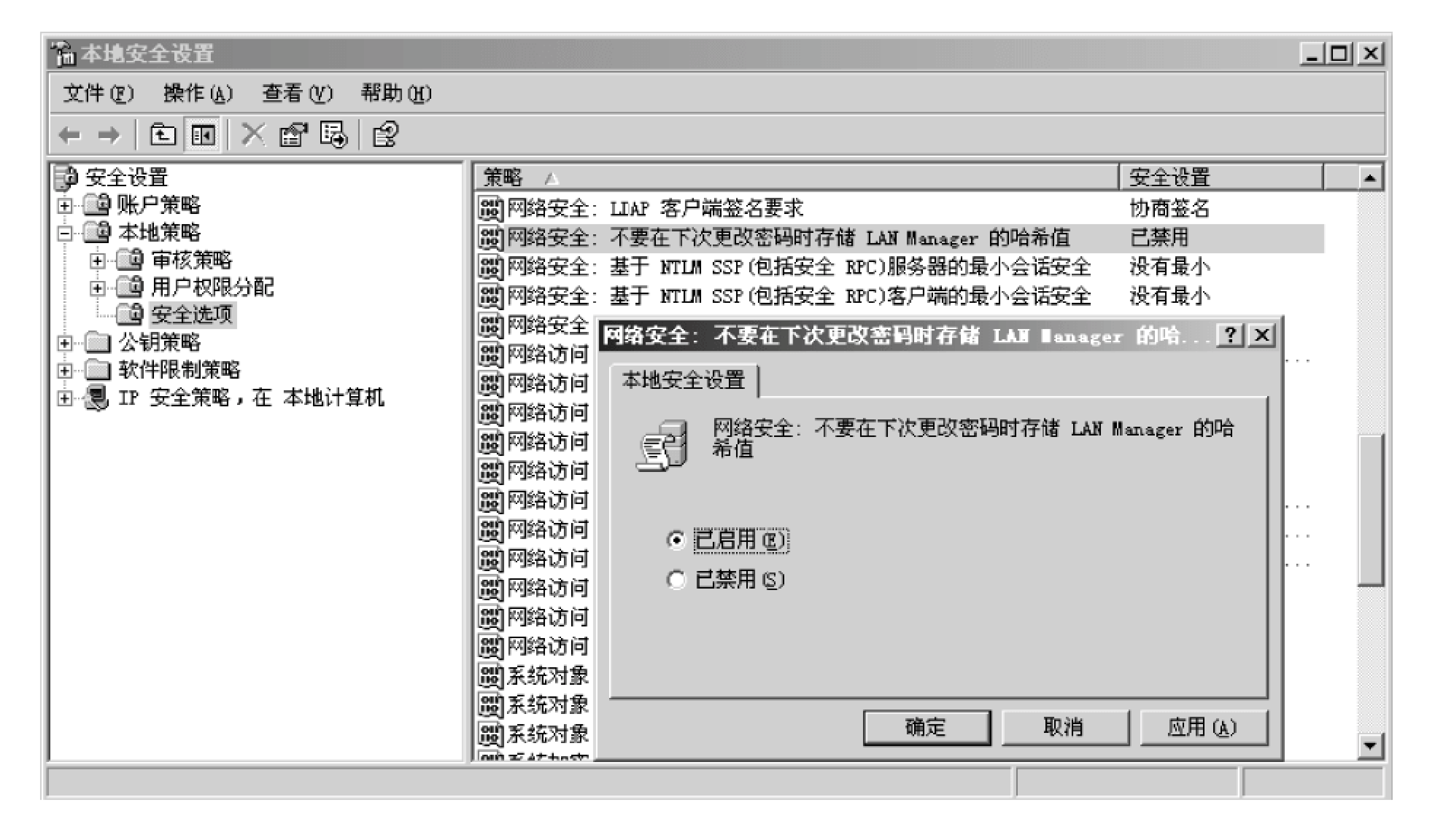


图 7-29 “安全选项”设置

(3) 利用账户安全策略进行安全防护

因为密码破解软件利用暴力破解、黑客字典等方法破解系统账户密码，只要有足够长的时间，可以破解任何密码，因此使用账户安全策略可以增加口令破解难度，有效地进行安全防护。具体操作步骤如下：

① 选择“开始”→“运行”菜单项，打开“运行”对话框。在“打开”下拉列表文本框中输入“secpol.msc”，然后单击“确定”按钮。

② 在本地安全设置中，选择“安全设置”→“账户策略”→“密码策略”菜单项。

③ 在右侧窗口双击“密码必须符合复杂度要求”，在弹出的对话框中选择“已启用”，然后单击“确定”按钮，如图 7-30 所示。

启用该策略后，新建账户密码必须满足复杂度要求，即密码不得包含账户名或用户全名的一部分，密码长度至少为 6 位字符，密码必须包含英文大写字母、英文小写字母、数字、非字母符号(例如￥、%、&、*、~、! 等)4 类中的 3 类。

如此设置后，仍然不能完全抵抗使用黑客字典的暴力破解法，还需要设定账户锁定策略，操作步骤如下：

① 在本地安全设置中，选择“安全设置”→“账户策略”→“账户锁定策略”菜单项。

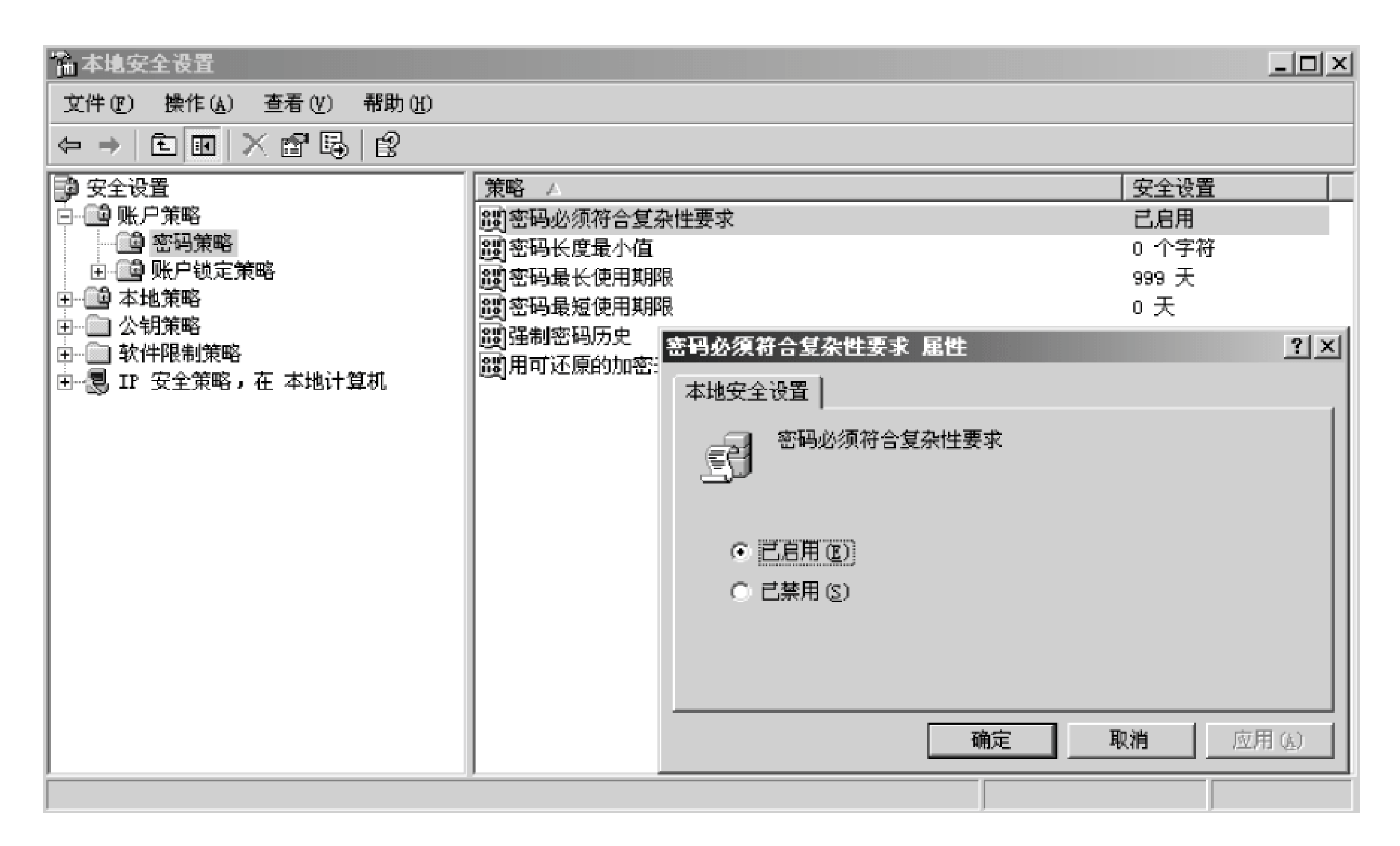


图 7-30　“密码策略”设置

② 在右侧窗口双击“账户锁定阈值”，在弹出的对话框中选择“3”，然后单击“确定”按钮，如图 7-31 所示。

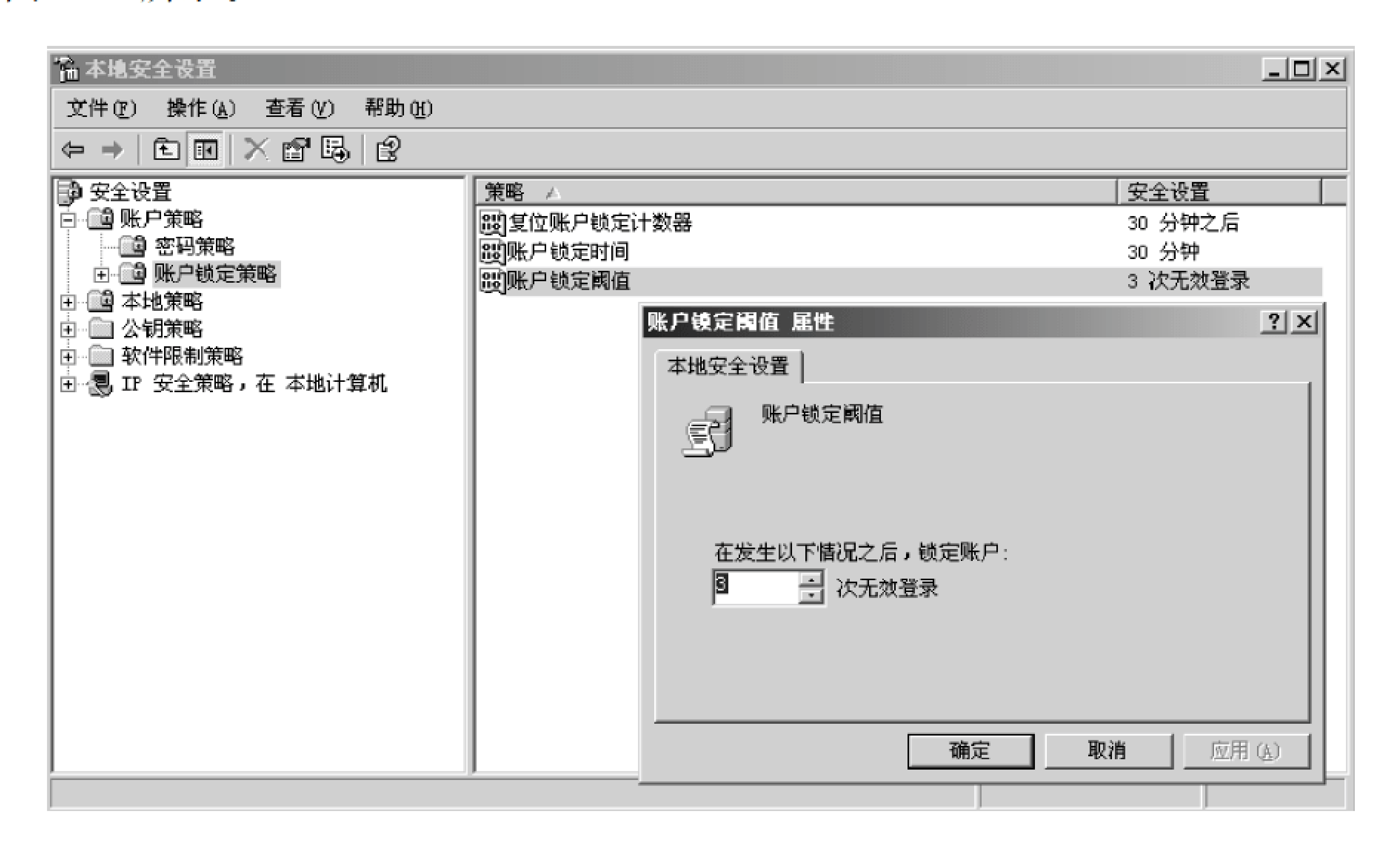


图 7-31　“账户锁定阈值”设置

还有一些技巧有助于维护系统的安全性，如下所示。

① 右击“我的电脑”，然后选择“管理”菜单，在“计算机管理”→“系统工具”→“本地用户和组”→“用户”中把 Administrator 账户重新命名，如图 7-32 所示。

② 再创建一个名为“Administrator”的本地账户，并将其权限设置成最低，并加上一个超过 10 位的超级复杂的密码。

③ 在计算机管理单元中查看系统的活动账户列表，禁用所有的非活动账户，特别是“Guest”，删除或者禁用不再需要的账户。



图 7-32　Administrator 账户重新命名

7.5　常见问题解答

1. NTFS 的磁盘格式与 FAT、FAT32 有什么区别？

答：FAT 最早是 DOS 所支持的文件系统，比较古老。它最大支持 4GB 分区，文件的存储效率和管理功能都比较低。FAT32 支持磁盘分区从 512MB 到 2TB，文件最大限制为 4GB。而 NTFS 支持磁盘分区从 100MB 到 2^{64}B，推荐最大分区是 2TB，支持文件和文件夹级的安全；可防止未授权用户访问文件或文件夹，支持文件压缩和加密功能，可以限制用户在某个分区使用空间，并能自动修复磁盘错误。

2. 如何进行分区转换？

答：FAT/FAT32 可以在不破坏数据的情况下转换成 NTFS，转换命令如下：

Convert <驱动器号：> /fs:ntfs [/可选参数]

但是，NTFS 不能转换成 FAT/FAT32。NTFS 到 FAT 的唯一办法就是先备份数据，然后重新格式化为 FAT/FAT32 分区，再将备份的数据恢复到新的 FAT/FAT32 分区中。

7.6　过关练习

一、选择题

Windows Server 2003 的 Administrator 账户的 RID 是(　　)。

A. 500　　B. 501　　C. 1000　　D. 1001

二、填空题

Windows Server 2003 安全模型的主要功能是________和________。

三、简答题

1. 简述 Windows Server 2003 主要包含的 6 个安全元素。
2. 简述安全标识符的含义及其作用。

四、实操题

1. 使用 LC5 审计你的本地账户，看是否安全。
2. 你有几种方法导出系统的 SAM？

工作任务八

注册表的管理

8.1 用户需求与分析

Windows 的注册表(Registry)是一个庞大的数据库,它包含了 Windows 运行期间不断引用的信息,存储着软、硬件的有关配置和状态信息,应用程序和资源管理器外壳的初始条件、首选项和卸载数据;计算机整个系统的设置和各种许可,文件扩展名与应用程序的关联,硬件的描述、状态和属性;计算机性能记录和底层的系统状态信息,以及各类其他的数据。从 Windows 启动过程到登录、应用程序的运行,Windows 中进行的所有操作都需要注册表的信息作为后盾,所以注册表的管理在网络管理员的系统维护中至关重要。

8.2 预 备 知 识

8.2.1 注册表的组成

从一般用户的角度看,注册表系统由注册表数据库和注册表编辑器两部分组成。注册表编辑器是专门编辑注册表的程序,负责注册表的浏览、编辑和修改。注册表编辑器与资源管理器相似,也是目录结构。但资源管理器中的目录是文件夹,而注册表中的目录是“键(key)”。在注册表编辑器中,最上面的键叫“根键”,里面包含的叫“子键”。单击根键前面的加号,就能展开属于这个根键的子键。

注册表编辑器的左侧窗口显示的是目录结构,右侧窗口显示的是与左侧窗口中的键相关的设定值、命令等。所有的注册表键都有“默认”项,每个值分为“名称”、“类型”和“数据”3 个部分,这种直观的结构体系也称为注册表的逻辑结构。

Windows 2003/XP 的注册表由 5 个根键组成。下面介绍每个根键的内容和含义,如表 8-1 所示。

表 8-1 注册表的 5 个根键

名 称	含 义	内 容
HKEY_CLASSES_ROOT	种类_根键	存有系统中所有的文件类型标识和基本操作标识
HKEY_CURRENT_USER	当前_用户键	存有当前用户配置文件和设置信息
HKEY_LOCAL_MACHINE	定位_机器键	存有计算机安装的硬件和软件的所有相关设置内容,以及硬件和硬件驱动程序的设置信息
HKEY_USERS	用户键	存有所有用户信息,包括动态加载的用户配置文件和默认的配置文件
HKEY_CURRENT_CONFIG	当前_配置键	存有本地计算机系统使用的硬件配置信息

8.2.2 注册表值的数据类型

注册表值采用了多种数据形式来存储设置。在注册表编辑器的右侧窗口中，“类型”显示的项目就是所属值的数据形式。经常使用的值的数据形式有字符串值、二进制值、DWORD值、多字符串值和可扩充字符串值等，如表8-2所示。

表8-2 注册表值的数据类型

数据类型	功能
DWORD值	DWORD表示双词(Double Word)，表示的类型为REG_DWORD。词是能表示0～65535范围内的16位数，因此DWORD是由两个16位值组成的32位数值。DWORD能表示2^{32}，也就是40亿以上的数据，但大部分情况下用来表示“真(1)”和假“(0)”
多字符串值	多种UNICODE的字符串集合，类型是REG_MULTI_SZ，能把多种内容显示为数据
字符串值	字符串类型的数据类型，表示为REG_SZ。这里的S是指“字符串(String)”，Z表示“以0组成的字节结束”
二进制值	用0和1表示的二进制数据类型，类型是REG_BINARY
可扩充字符串值	XP中使用多个系统定义变量，这些变量可以在BAT文件或控制面板的系统环境变量中设定，在注册表编辑器中显示为REG_EXPAND_SZ类型

8.2.3 注册表的打开方式

注册表采用命令行方式打开。选择“开始”→“运行”菜单项，在“打开”下拉列表文本框中输入“regedit”命令并按“Enter”键，可以打开注册表窗口。

8.3 方案设计

方案设计如表8-3所示。

表8-3 方案设计

任务名称	注册表的管理
任务分解	1. 关闭默认共享 (1) 防范IPC$攻击 (2) 修改注册表，关闭默认共享 2. 设置Windows的自动登录 3. 清除系统中随机启动的木马 4. 清除恶意代码 (1) 删除开机自动弹出的网页 (2) 删除开机自动弹出的恶作剧对话框 (3) 修改IE首页 (4) 修改IE右键菜单 5. 防止SYN洪水攻击

续表

能力目标	1. 能通过修改注册表达到防范 IPC＄攻击的目的 2. 能通过修改注册表关闭默认共享 3. 能通过修改注册表达到自动登录到计算机的目的 4. 能手动清除隐藏在系统中随机启动的木马 5. 能通过修改注册表删除开机自动弹出的网页 6. 能通过修改注册表删除开机自动弹出的恶作剧对话框 7. 能手动修改被篡改的 IE 首页 8. 能手动修改 IE 右键菜单项 9. 能通过修改注册表防范 SYN 洪水攻击
知识目标	1. 了解注册表的组成 2. 熟悉注册表值的数据类型 3. 掌握注册表的打开方式
素质目标	1. 培养良好的职业道德 2. 树立较强的安全意识 3. 培养职业兴趣，以及爱岗敬业、热情主动的工作态度 4. 具有可持续发展能力 5. 树立较强的安全、节约、环保意识

8.4 任务实施

8.4.1 任务1：关闭默认共享

1. 任务目标

在默认安装 Windows 系统的情况下，为了管理方便，所有的硬盘都是隐藏共享的。一般默认共享的目录只有系统管理员才能够在网络中查看到，因为在共享名称旁加了“＄”符号，除非别人知道这个共享，否则将无法找到该共享的文件。虽然对其访问需要超级用户的密码，但这是潜在的安全隐患，因此从服务器的安全考虑，最好关闭这个“默认共享”，以保证系统的安全。

2. 工作任务

（1）防范 IPC＄攻击；

（2）修改注册表，关闭默认共享。

3. 工作环境

一台预装 Windows Server 2003/XP 的主机。

4. 实施过程

（1）防范 IPC＄攻击

通过修改注册表，达到防范 IPC＄攻击的目的，具体步骤如下：

① 打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa，如图 8-1 所示。

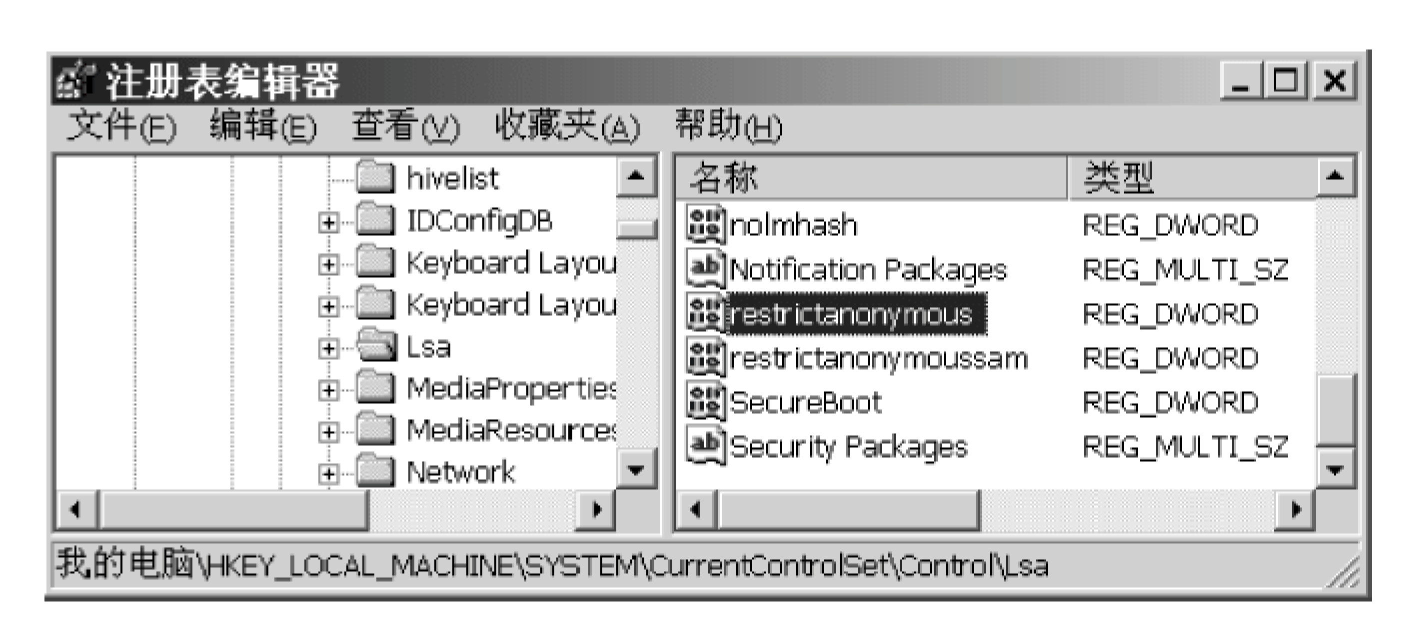


图 8-1 打开注册表编辑器(1)

② 在该子键右边窗格中找到并双击打开“restrictanonymous”键值项，将“数值数据”文本框里的数值修改为“1”，然后单击“确定”按钮保存，如图 8-2 所示。



图 8-2 修改“restrictanonymous”键值

(2) 修改注册表，关闭默认共享

要关闭 C＄、D＄ 和 admin＄ 等类型的默认共享，按照以下步骤来操作。

① 打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lamanserver\parameters，如图 8-3 所示。

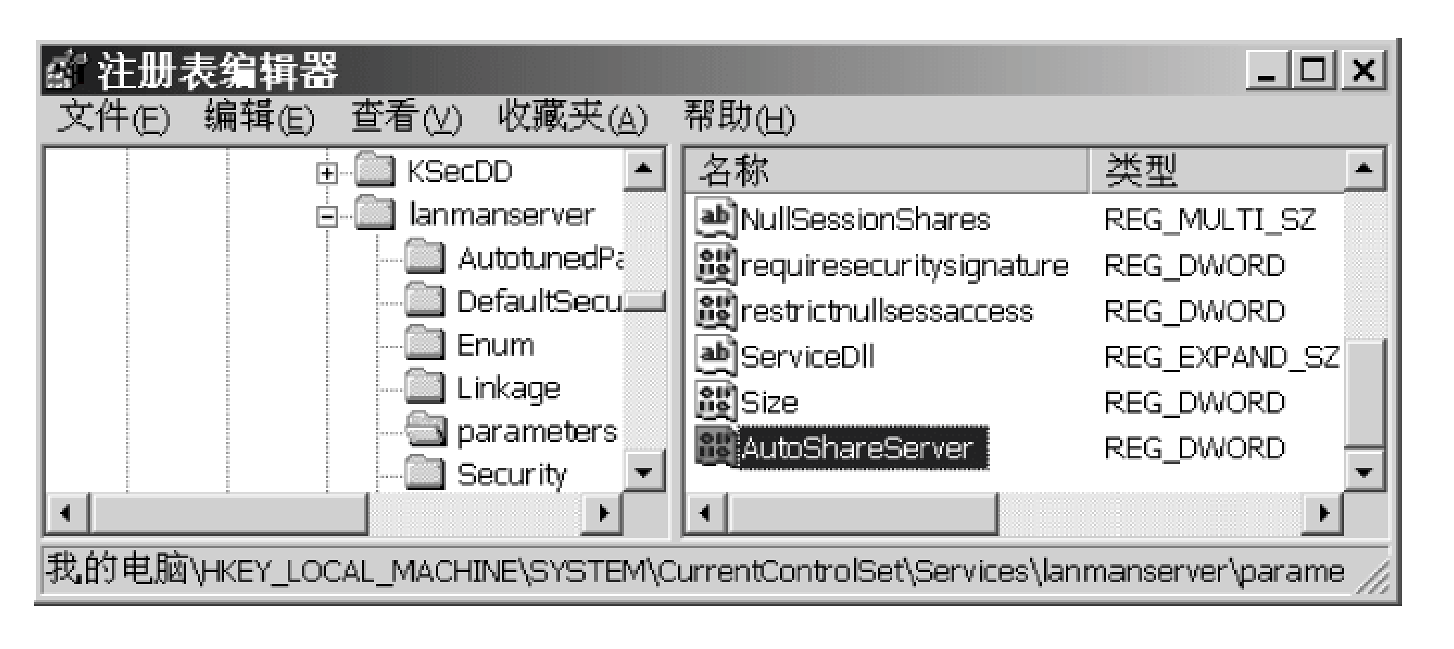


图 8-3 打开注册表编辑器(2)

② 在该子键右边窗格中找到并双击打开“AutoShareServer”键值项，将“数值数据”文本框里的数值修改为“0”，然后单击“确定”按钮，如图 8-4 所示。



图 8-4 修改“AutoShareServer”键值

③ 如果找不到“AutoShareServer”键值项，在右侧窗格中右击，然后在弹出的快捷菜单中选择“新建”→“DWORD”菜单项，再在新建项上右击，将其重新命名为“AutoShareServer”，类型为“REG_DWORD”，值为“0”。

8.4.2 任务 2：设置 Windows 的自动登录

1. 任务目标

如果计算机被黑客监控了，在登录 Windows 时账号密码有可能外泄，可通过设置注册

表，允许用户绕过 Windows 系统的登录对话框，自动登录到计算机和网络中。

2. 工作任务

设置 Windows 的自动登录。

3. 工作环境

一台预装 Windows Server 2003/XP 的主机。

4. 实施过程

通过修改注册表，达到自动登录到计算机的目的，具体步骤如下：

(1) 打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon，如图 8-5 所示。

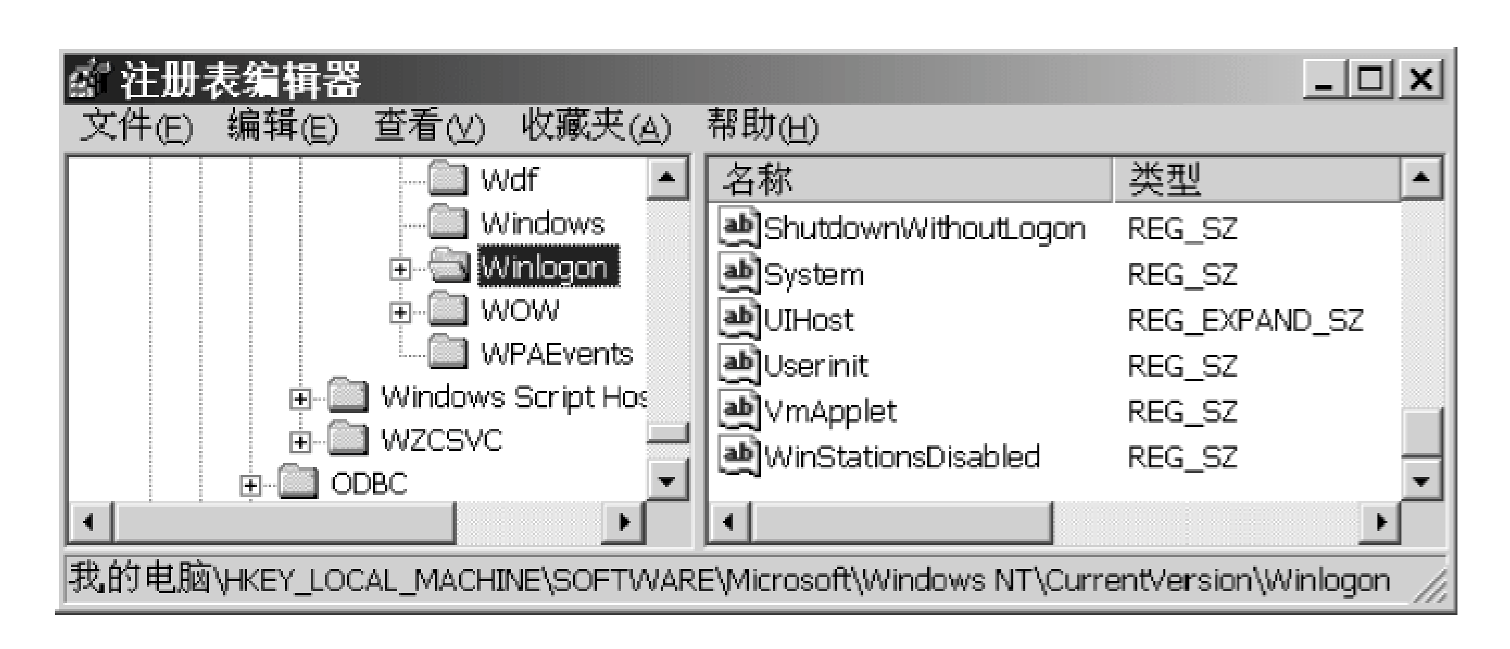


图 8-5 打开注册表编辑器(3)

(2) 右击 Winlogon 子键创建 3 个"字符串值"，并将其分别命名为 DefaultDomainName、DefaultUserName 和 DefaultPassword，如图 8-6 所示。

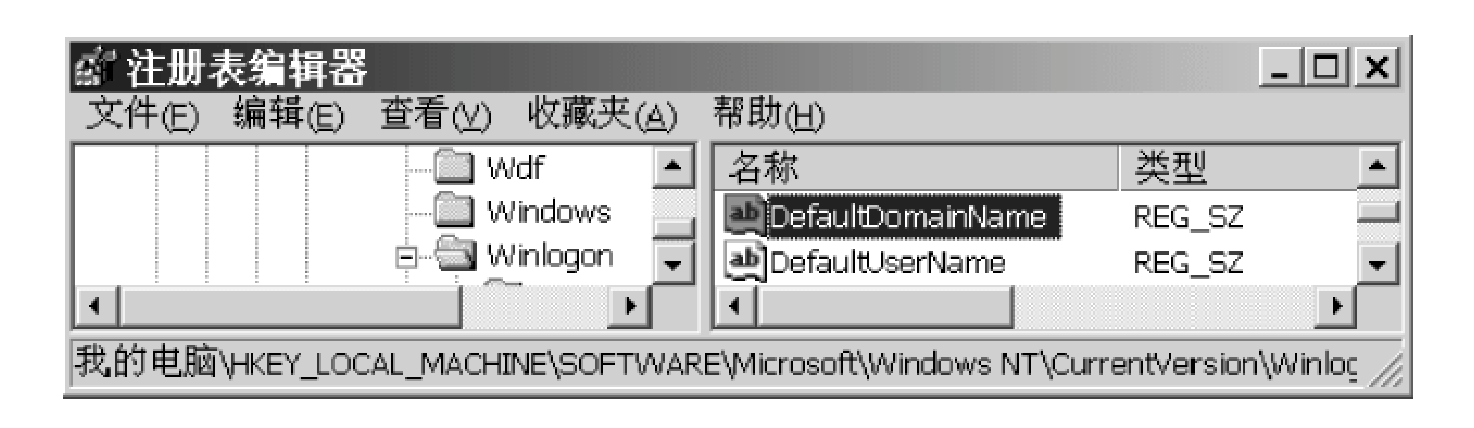


图 8-6 创建新键值项

(3) 上步创建的 3 个键值项分别为用户所在的域名、登录用户名和密码。依次编辑键值，然后单击"确定"按钮保存，如图 8-7 所示。

(4) 再新建一个名为"AutoAdminLogon"的字符串值并将键值设置为"1"，已激活自动登录，单击"确定"按钮保存，如图 8-8 所示。

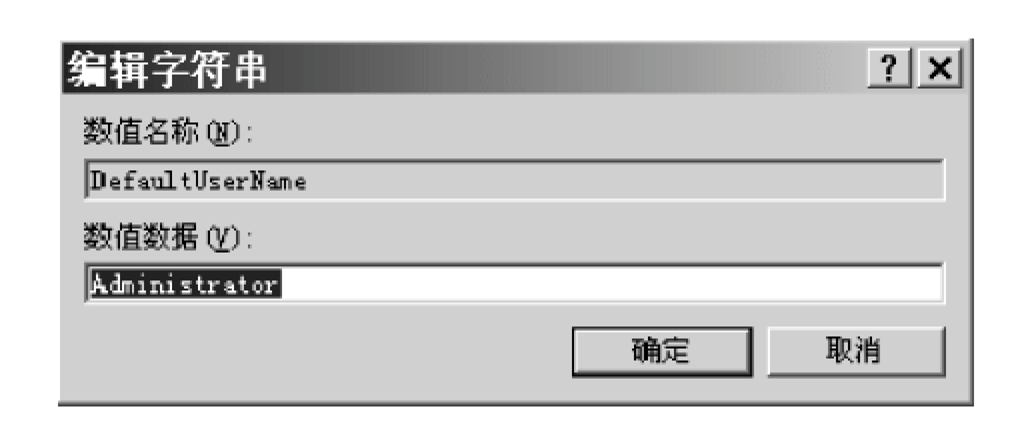


图 8-7 设置登录用户名

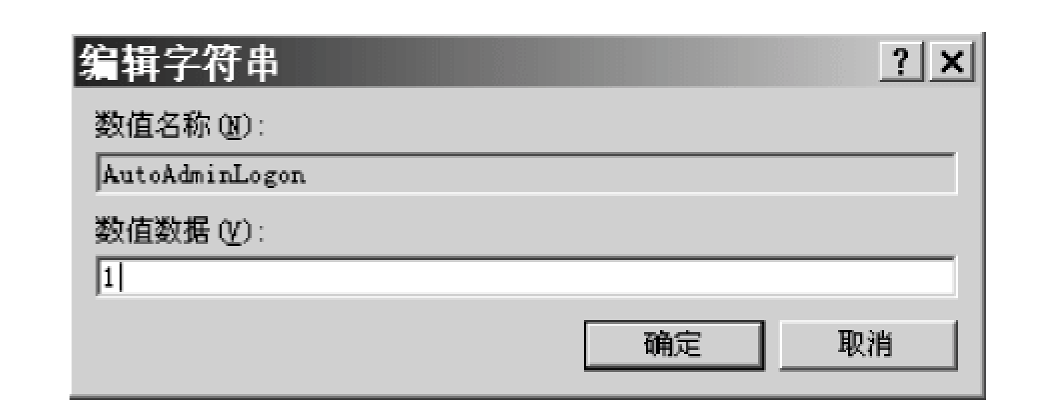


图 8-8 设置键值(1)

8.4.3 任务3：清除系统中随机启动的木马

1. 任务目标

木马通常将自身隐藏在系统中某个不起眼的角落里，并且将自己伪装成“面貌普通”的文件，一旦用户不小心运行了该木马的服务端，它将在用户的计算机上立即开始工作，通过端口与客户端连接，黑客就可以通过某个端口连接到该计算机上进行攻击。通过注册表的设置可以清除系统中随机启动的木马。

2. 工作任务

清除系统中随机启动的木马。

3. 工作环境

一台预装 Windows Server 2003/XP 的主机。

4. 实施过程

在注册表中自动启动的木马往往隐藏在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run、HKEY_LOCAL_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run、HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run 等子键中。删除这些木马的具体操作步骤如下：

(1) 打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，如图 8-9 所示。

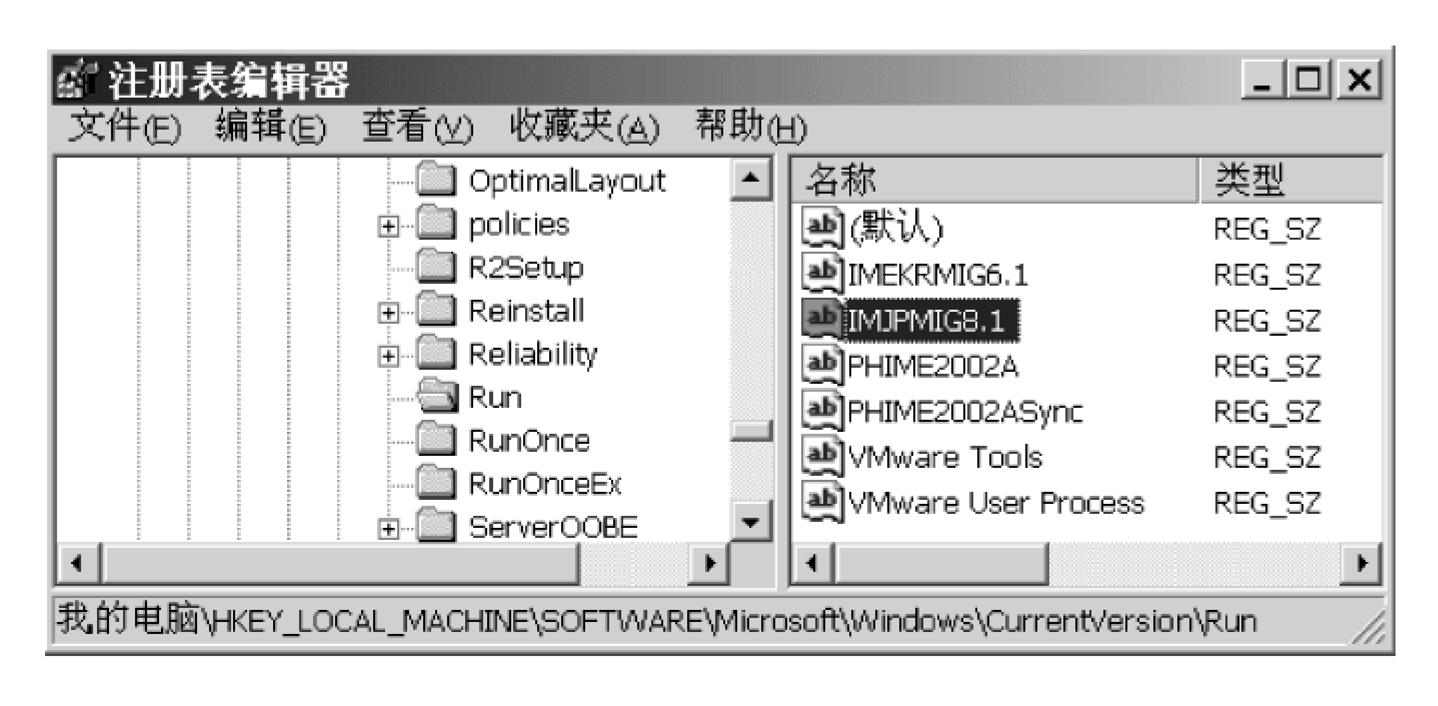


图 8-9 打开注册表编辑器(4)

(2) 在右边的窗格中查找，看是否有可疑的自动启动文件，扩展名为.exe。

(3) 按 Ctrl+F 快捷键弹出“查找”对话框，然后在查找目标文本框中输入在第(2)步发现的可疑可执行文件。单击“查找下一个”按钮，将找到所有和这个键值一样的程序，将其删除。

(4) 退出注册表，重启计算机。

注意： 有些木马程序产生的文件很像系统自带的文件，有时只有一个字母的差别。

8.4.4 任务4：清除恶意代码

1. 任务目标

Windows 系统启动的同时就开始与注册表的数据信息进行相互交换，并且在计算机使

用的过程中，系统不断与注册表中保存的数据信息进行相互交换。因此当用户在浏览互联网或下载软件、资料时，都面临着由于系统漏洞导致系统遭受各种恶意攻击的风险，一旦感染了恶意代码，都可能致使自动弹出恶意网站和对话框，甚至有时 IE 浏览器的首页和右键菜单被篡改得面目全非，而几乎所有的网页恶意代码都是利用注册表来实现操作的。

2. 工作任务

(1) 删除开机自动弹出的网页；

(2) 删除开机自动弹出的恶作剧对话框；

(3) 修改 IE 首页；

(4) 修改 IE 右键菜单。

3. 工作环境

一台预装 Windows Server 2003/XP 的主机。

4. 实施过程

(1) 删除开机自动弹出的网页

最常见的恶意代码是开机即自动弹出网页，这是注册表项被恶意添加网址所致。用户可以打开注册表编辑器，展开下面两个子键，如果发现这两个子键下的某个键值项的键值是弹出网页的网址，将键值删除，然后重启计算机。这两个子键分别是 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce。

在右侧窗格中将 url、html、htm、asp、aspx 或者 php 等网址属性的键值全部删除。这种恶意代码往往会对注册表的不同键值进行多处修改，删除一处可能还不能完全将其清除，因此用户可以使用注册表编辑器的查找功能来搜索目标，并将其删除。

(2) 删除开机自动弹出的恶作剧对话框

某些恶意代码会修改注册表的某些键值项，让用户在开机的时候弹出一些莫名其妙的对话框，这个子键为 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon。

这种对话框看起来很有危险性，其实只是一个恶作剧。如果不喜欢别人使用自己的计算机，可以利用这个策略来警示不受欢迎的“客人”。具体操作步骤如下：

① 打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Winlogon，如图 8-10 所示。



图 8-10　打开注册表编辑器(5)

② 在 Winlogon 的右侧窗格中找到两个键值项 LegalNoticeCaption 和 LegalNoticeText，然后双击打开并输入警示性文字，再单击“确定”按钮，如图 8-11 和图 8-12 所示。

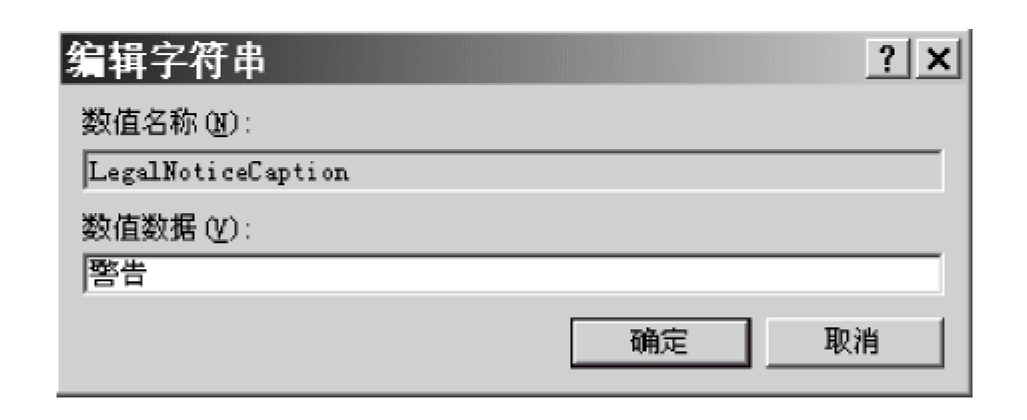


图 8-11　在“LegalNoticeCaption”中设置警示性文字



图 8-12　在“LegalNoticeText”中设置警示性文字

③ 关闭注册表编辑器后重启计算机，在出现登录对话框之前会弹出一个警示框。单击“确定”按钮将仍然进入系统，不会有什么影响。如果要取消该设置，把键值删除即可。

(3) 修改 IE 首页

① 打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main。

② 在右侧窗格选中“Start Page”选项，然后右击，在弹出的快捷菜单中选择“修改”菜单项。

③ 打开“编辑字符串”对话框，将“数值数据”文本框中的内容设置为想要的首页，然后单击“确认”按钮。

(4) 修改 IE 右键菜单

① 打开注册表编辑器，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MenExt。

② 选中含有恶意代码的 IE 右键菜单项，然后右击，从弹出的快捷菜单中选择“删除”菜单项。

8.4.5 任务 5：防止 SYN 洪水攻击

1. 任务目标

SYN 攻击属于 DoS 攻击的一种，它利用 TCP 协议缺陷，通过发送大量半连接请求消耗 CPU 和内存资源。SYN 攻击除了影响主机外，还危害路由器、防火墙等网络系统。

SYN 攻击的工作原理是当服务器接收到连接请求时，服务器将此请求信息加入未连接队列中，并发送请求包给客户端；当服务器未收到客户端的确认包时，将会重发请求包，直到超时，才将该信息从未连接队列中删除。配合 IP 欺骗 SYN 的攻击效果很好。客户端利用伪装大量不存在的 IP 地址向服务器不断发送 SYN 包，服务器回复确认包后，等待客户的确认，因为源地址是不存在的，因此服务器需要不断重发直至超时。伪装的 SYN 包长时间占用未连接队列，致使正常的 SYN 包被丢弃，目标系统运行缓慢，甚至处于瘫痪状态。

SYN 攻击不管目标主机是什么系统，只要这些系统打开了 TCP 服务就可以实施。为了防范 SYN 攻击，Windows 2000 以上的版本都在 TCP/IP 协议内嵌了 SynAttackProtect 机制，通过关闭某些 Socket 选项，增加额外的连接指示并减少超时时间，使系统能处理更多 SYN 连接。但在默认情况下，Windows 并不支持 SynAttackProtect 保护机制，需要在注册表中做出相应的修改才行。

2. 工作任务

防止 SYN 洪水攻击。

3. 工作环境

一台预装 Windows Server 2003/XP 的主机。

4. 实施过程

(1) 打开注册表编辑器,依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters,如图 8-13 所示。

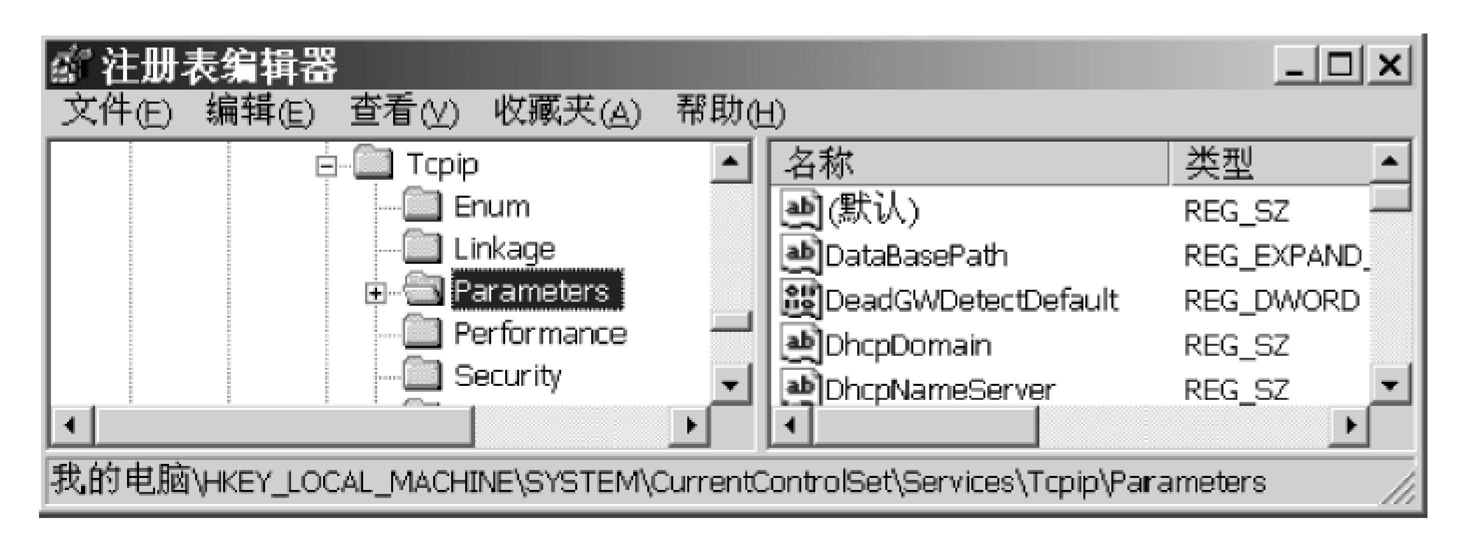


图 8-13　打开注册表编辑器(6)

(2) 在右侧窗格空白处右击,然后从弹出的快捷菜单中单击“新建 DWORD 值”,将新创建的 DWORD 值命名为 SynAttackProtect,如图 8-14 所示。

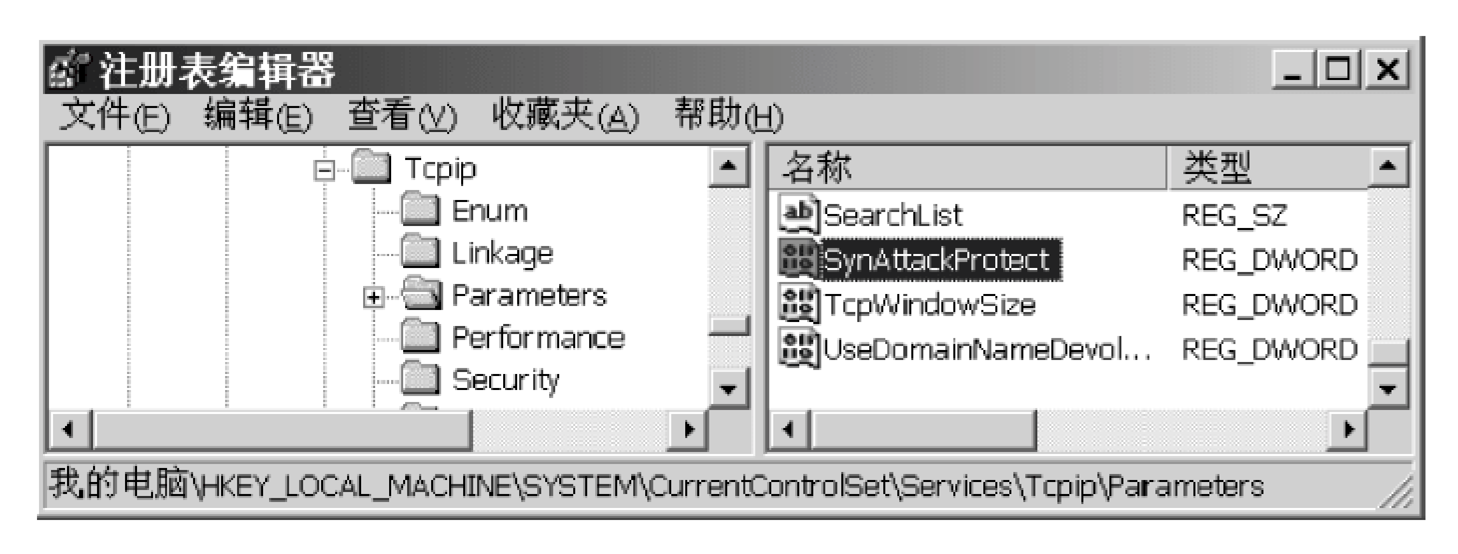


图 8-14　新建键值项

(3) 双击打开新创建的 SynAttackProtect 键值项,然后将“数值数据”文本框内的数字修改为“2”,单击“确定”按钮保存,如图 8-15 所示。



图 8-15　设置键值(2)

(4) 用同样的方法创建 6 个 DWORD 键值项,分别是 EnablePMTUDiscovery 键值为 0、NoNameReleaseOnDemand 键值为 1、EnableDeadGWDetec t 键值为 0、KeepAliveTime 键值为 300000、PerformRouterDiscovery 键值为 0、EnableCMPRedirect 键值为 0。

8.5 常见问题解答

1. 恶意代码常利用的注册表启动项有哪些?

答:恶意代码常利用的注册表启动项有以下几种。

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run;

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce;

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServics;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon。

2. 如何利用注册表屏蔽445端口?

答:在命令行窗口输入"regedit"命令,打开注册表编辑器,然后展开到HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\NetBT\Parameters,并添加一个键值,名为"SMBDeviceEnabled",类型为"REG_DWORD",值为"0",修改完毕后重启计算机即可生效。

8.6 过关练习

一、选择题

在Windows"运行"窗口中输入(　　)命令,可以查看和修改注册表。

A. cmd　　B. mmc　　C. autoexe　　D. regedit

二、简答题

如何备份和还原注册表?

工作任务九

组策略的设置

9.1 用户需求与分析

所谓组策略，就是基于组的策略。它以 Windows 中的一个 MMC 管理单元的形式存在，可以帮助系统管理员针对整个计算机或者特定用户来设置多种配置，包括桌面配置和安全配置。通过使用组策略，用户可以设置各种软件、计算机和用户策略。

9.2 预备知识

9.2.1 组策略的作用

组策略是管理员为计算机和用户定义的，用来控制应用程序、系统设置和管理模板的一种机制。如同一个庞大的数据库，它保存着 Windows 系统中与系统、应用软件配置相关的信息。随着 Windows 功能越来越丰富，以及用户安装在计算机中的软件程序越来越多，注册表中的相关信息越来越多。

组策略是修改注册表中的配置的一个有效工具。它使用更加完善的管理组织方法，对各种对象中的配置进行管理和设置，远比手动修改注册表更加方便、灵活，功能更加强大。在注册表中，很多信息都是可以由用户自定义设置的，但这些信息发布在注册表的各个角落，如果是手动配置，会非常困难和繁杂。而组策略将系统重要的配置功能汇集成各种配置模块，供管理人员直接使用，从而达到方便管理计算机的目的。

组策略是介于控制面板和注册表之间的一种修改系统与设置程序的工具，利用它可以修改 Windows 的桌面、开始菜单、登录方式、组件、网络及 IE 浏览器等许多设置。通常情况下，像一些常用的系统、外观及网络设置等，用户可以在控制面板中修改，但用户对此并不满意，因为通过控制面板能修改的设置太少；水平高一点的用户可以用修改注册表的方法来设置，但是注册表中涉及的内容太多，修改起来不方便。组策略正好介于两者之间，涉及的内容比控制面板多，安全性和控制面板一样高，而条理性、可操作性比注册表强，因此成为网络管理员管理系统的首选。

9.2.2 组策略的打开方式

组策略的打开方式有两种。

1. 方式一：使用命令行

选择“开始”→“运行”菜单项，在“打开”下拉列表文本框中输入“gpedit. msc”命令并按

“Enter”键，打开组策略窗口。在该窗口的左边窗格中，用户可以看到两个选项，即“计算机配置”和“用户配置”。

2. 方式二：利用 MMC 控制台

MMC 是 Microsoft Management Console 的缩写，它是 Windows 中一个很重要的系统管理工具，组策略实际上就是一个预置在 Windows 中的 MMC，因此用户可以将其作为独立的 MMC 来打开。选择“开始”→“运行”菜单项，在“打开”下拉列表文本框中输入“MMC”命令并按“Enter”键，打开“控制台”窗口，即 Microsoft 管理控制台。在该窗口中选择“文件”→“添加/删除管理单元”菜单项，在打开的“添加/删除管理单元”对话框中切换到“独立”选项卡，然后单击“添加”按钮，打开“添加独立管理单元”对话框。可以看到，在“可用的独立管理单元”列表框中显示了计算机中早已预置好的独立管理单元，找到并选中“组策略对象编辑器”选项，然后单击“添加”按钮，如图 9-1 所示。

打开“选择组策略对象”对话框，默认情况下，该组策略是为本地计算机设置的。如果用户想为其他计算机设置组策略，可以单击“浏览”按钮，在打开的“浏览组策略对象”对话框中选择相应的计算机。这里保持系统默认设置，即使用本地计算机。选中“当从命令行开始时，允许更改组策略管理单元的焦点。只有您保存该控制台的情况下，这点才可以起作用”复选框。当用户使用命令行打开“组策略”窗口时，用户可以更改其中的内容。最后单击“完成”按钮，如图 9-2 所示，返回“添加独立管理单元”对话框。单击“关闭”按钮将其关闭并返回“添加/删除管理单元”对话框，可以发现，“本地计算机策略”选项被添加在相应的列表框中。单击“确定”按钮，返回“控制台 1”对话框，此时可以发现打开了相应的组策略管理单元。





图 9-1 “添加独立管理单元”对话框



图 9-2 “选择组策略对象”对话框

注意：如果因为误操作导致无法通过第一种方法进入组策略编辑器，可以在计算机重启的时候按住 F8 键，再选择带命令行的安全模式，然后在命令行窗口输入“mmc”进入控制台，用户可以更改其中的内容。

9.3 方案设计

方案设计如表 9-1 所示。

表 9-1　方案设计

任务名称	组策略的设置
任务分解	1. 组策略的开机策略 (1) 设置密码策略 (2) 设置账户锁定策略 2. 组策略的安全设置 (1)“桌面”设置 (2)“任务栏”和“开始”菜单设置 (3) IE 设置 (4) Windows 高级功能设置 3. 系统的安全管理 (1) 禁止在登录前关机 (2) 不显示上次登录的用户名
能力目标	1. 能设置密码策略 2. 能设置账户锁定策略 3. 能隐藏桌面的系统图标 4. 能在退出时不保存桌面设置 5. 能屏蔽“清理桌面向导”功能 6. 能设置满足需要的“任务栏”和“开始”菜单 7. 能禁止系统“注销”和“关机” 8. 能用组策略保护个人文档隐私 9. 能禁用网页的“新建”、“在新窗口中打开”等功能 10. 能限制 IE 浏览器的保存功能 11. 能禁用 IE 的“Internet 选项”控制面板 12. 能禁止修改 IE 浏览器的主页 13. 能自定义 IE 工具栏 14. 能实现远程关机 15. 能隐藏“我的电脑”中指定的驱动器 16. 能防止从“我的电脑”访问驱动器 17. 能禁止设置“文件夹选项” 18. 能防止访问控制面板，或禁用“添加/删除程序” 19. 能禁止使用命令提示符 20. 能禁止使用注册表编辑器 21. 能限制使用应用程序 22. 能禁止在登录前关机 23. 能不显示上次登录的用户名
知识目标	1. 熟悉组策略的作用 2. 掌握组策略的打开方式
素质目标	1. 树立较强的安全、节约、环保意识 2. 具有可持续发展能力 3. 培养良好的职业道德 4. 掌握网络安全行业的基本情况 5. 培养职业兴趣，以及爱岗敬业、热情主动的工作态度

9.4 任务实施

9.4.1 任务1：组策略的开机策略

1. 任务目标

用户可以使用组策略来对开机进行设置，以使自己的计算机和隐私更加安全、可靠。

2. 工作任务

(1) 设置密码策略；

(2) 设置账户锁定策略。

3. 工作环境

一台预装Windows Server 2003/XP的主机。

4. 实施过程

(1) 设置密码策略

密码是用户登录到系统的凭证。网络中存在一些别有用心的人，总是想尽方法以各种手段来破解用户密码，以达到不可告人的目的。密码起着比用户账号更加重要的作用。设置密码策略的步骤如下：

① 选择"开始"→"运行"菜单项，输入"gpedit.msc"后按"Enter"键，打开"组策略"窗口。在该窗口中依次展开"计算机配置"→"Windows设置"→"安全设置"→"账户策略"→"密码策略"，用户可以在右边窗格中看到6个账户锁定策略选项，分别是"密码必须符合复杂性要求"、"密码长度最小值"、"密码最长使用期限"、"密码最短使用期限"、"强制密码历史"和"用可还原的加密来存储密码"，如图9-3所示。

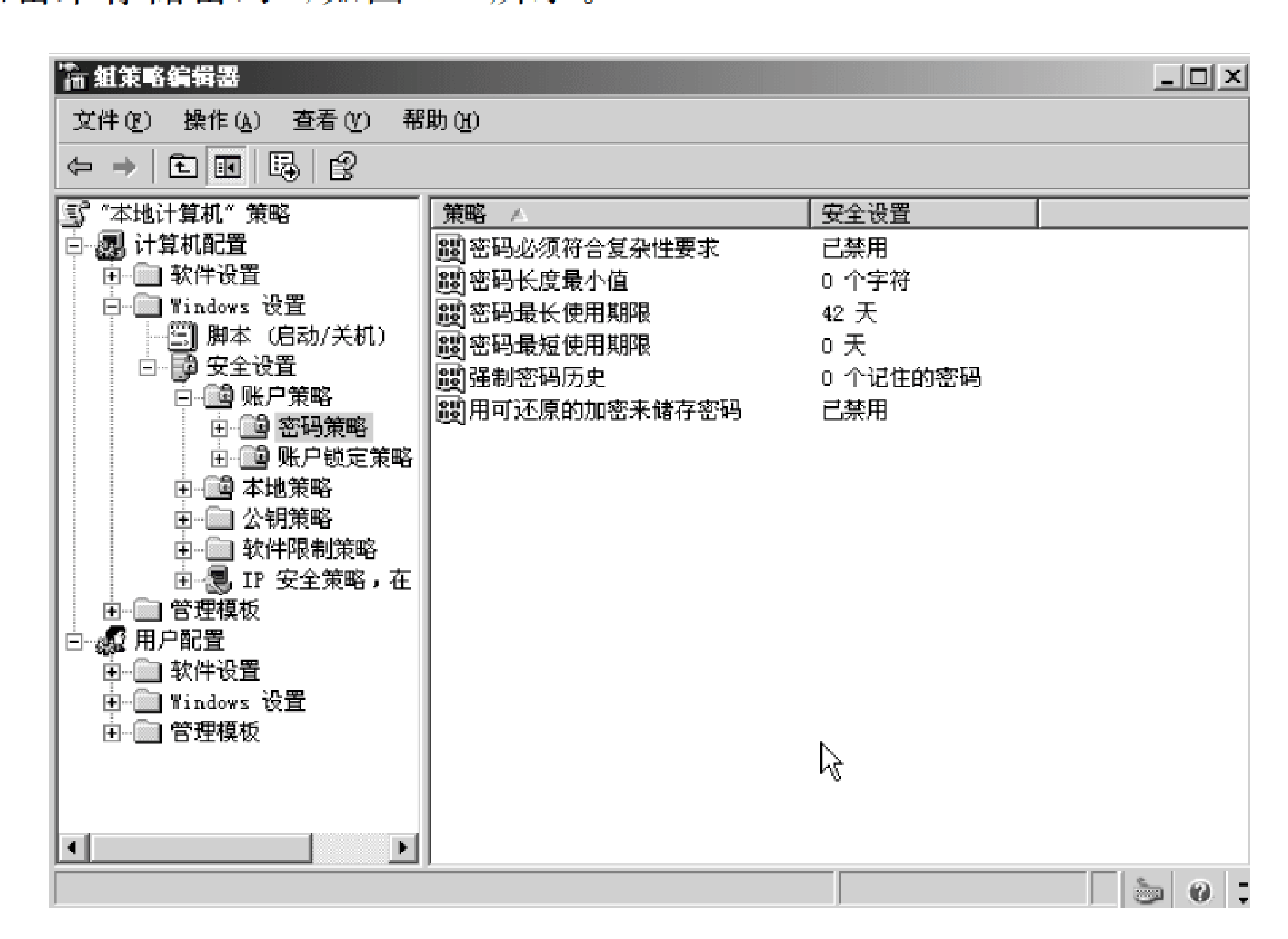


图9-3 "密码策略"设置

② 用户可以双击密码策略选项，打开相应的属性对话框，设置属性值。例如，双击“密码长度最小值”密码策略选项，然后设置数值，如图 9-4 所示。



图 9-4 “密码长度最小值 属性”对话框

表 9-2 中列出了这 6 个密码策略选项的说明。

表 9-2 密码策略选项说明

密码策略	说明
密码必须符合复杂性要求	启用该策略，密码必须满足： (1) 不包含全部或部分的账户名； (2) 长度至少为 6 个字符； (3) 包含英文大写字母、英文小写字母、基本数字和非字母字符中的 3 类； (4) 更改或创建密码时，会强制执行复杂需求
密码长度最小值	1～14，若设置为“0”，表示不需要密码
密码最长使用期限	1～999，若设置为“0”，表示密码永不过期
密码最短使用期限	1～999，若设置为“0”，表示允许立即更改密码
强制密码历史	0～24，确保旧密码不能继续使用
用可还原的加密来存储密码	除非应用程序有比保护密码信息更重要的要求，否则不必启用该策略

(2) 设置账户锁定策略

在默认情况下，用户在登录界面可以有很多次输入无效用户账号和密码的机会，这也为使用字典攻击的网络攻击者提供了快速破解用户账号和密码的机会，从而给用户的权益带来损害。为了解决这一问题，用户可以使用组策略设置账户锁定策略，将非法用户阻挡在系统之外。系统的 Administrator 账户即超级管理员账户不会因为账户锁定策略的设置而被锁定。设置账号锁定策略的具体操作如下：

① 选择“开始”→“运行”菜单项，输入“gpedit.msc”后按“Enter”键，打开“组策略”窗口。

② 在该窗口中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“账户锁定策略”，用户可以在右边窗格中看到 3 个账户锁定策略选项，分别是“复位账户锁定计数器”、“账户锁定时间”和“账户锁定阈值”，如图 9-5 所示。

③ 双击“账户锁定阈值”选项，打开“账户锁定阈值 属性”对话框。默认情况下，账户为不锁定状态，用户可以根据自己的实际情况进行设置(下限为 0，代表账户不设置锁定状态；

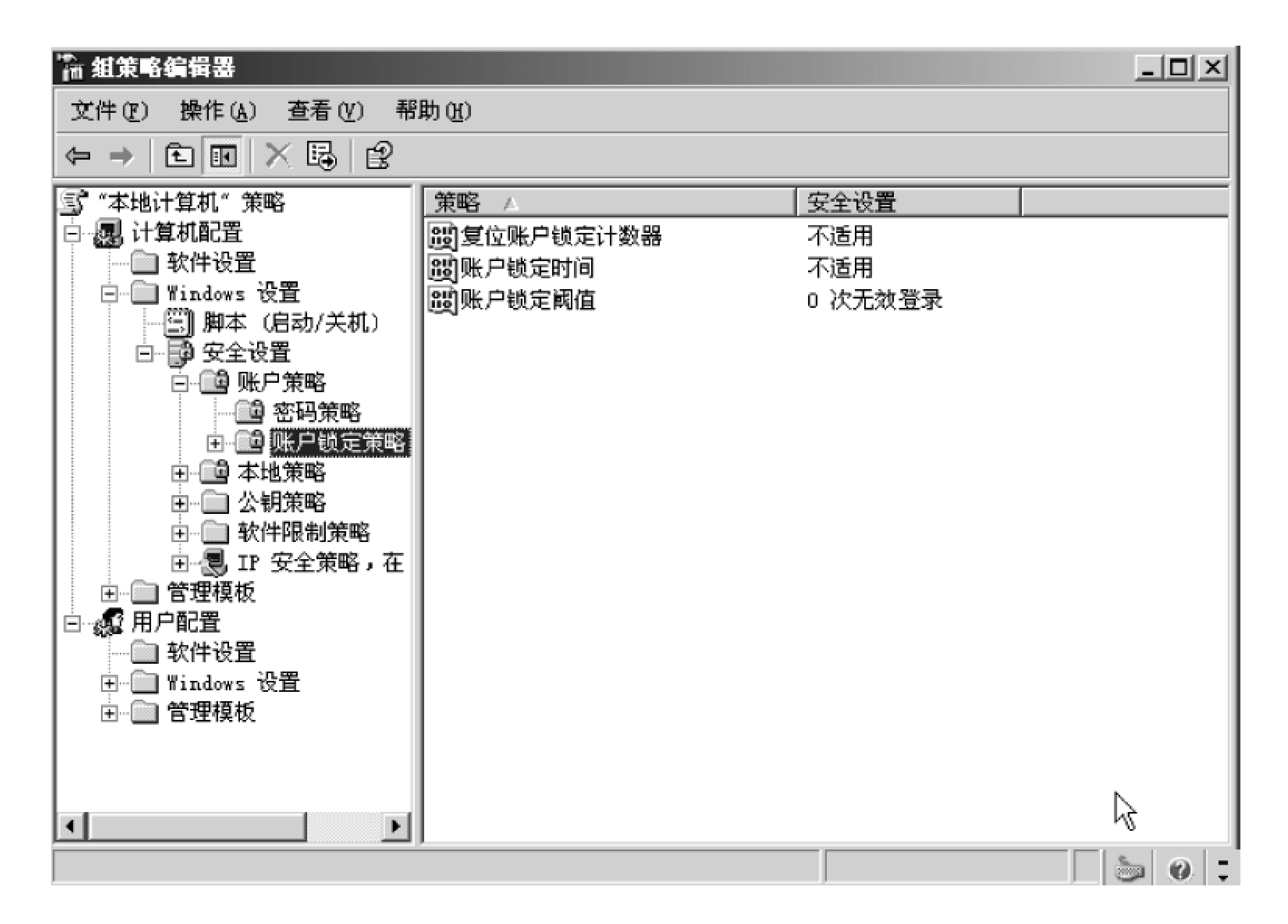


图 9-5 “账户锁定策略”设置

上限为 999 次，即经过 999 次无效输入以后，账户被设置为锁定状态）。

④ 例如设置成 3 次，然后单击“应用”按钮，将弹出“建议的数值改动”对话框。单击“确定”按钮后，其他两个策略选项的数值会自动被设置为被建议的数值，如图 9-6 所示。

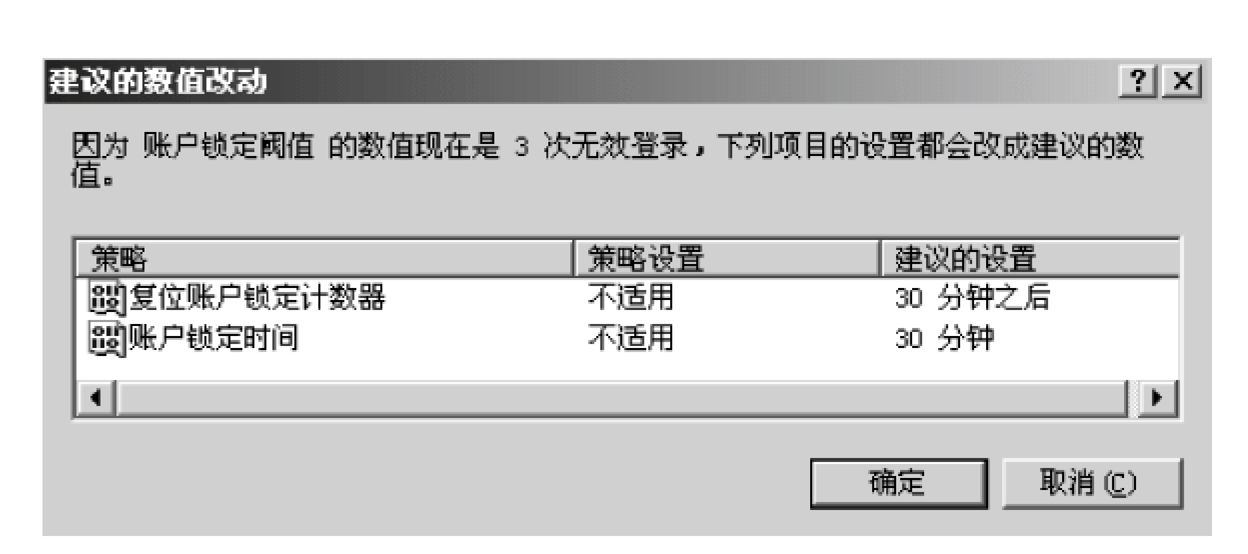


图 9-6 “建议的数值改动”对话框

如果用户不慎忘记了登录的用户名和密码，可以在进入登录界面时按下 Ctrl＋Alt＋Delete 组合键，启用 Administrator 账户来登录系统。

9.4.2 任务 2：组策略的安全设置

1. 任务目标

用户可以使用组策略设置开机，使自己的计算机和隐私更加安全、可靠。

2. 工作任务

（1）“桌面”设置；

（2）“任务栏”和“开始”菜单设置；

（3）IE 设置；

（4）Windows 高级功能设置。

3. 工作环境

一台预装 Windows Server 2003/XP 的主机。

4. 实施过程

(1)“桌面”设置

Windows 的桌面就像我们的办公桌一样,需要经常整理和清洁;组策略就如同我们的贴身秘书,让桌面管理工作变得易如反掌。

位置:组策略控制台→用户配置→管理模板→桌面。

① 隐藏桌面的系统图标(Windows 2000/XP/2003)

虽然通过修改注册表的方式可以实现隐藏桌面上的系统图标的功能,但这样比较麻烦,也有一定的风险。采用组策略配置的方法,可以方便、快捷地达到此目的。

比如要隐藏桌面上的“网上邻居”和“Internet Explorer”图标,只要在右侧窗格中将“隐藏桌面上‘网上邻居’图标”和“隐藏桌面上的 Internet Explorer 图标”两个策略选项启用即可,如图 9-7 所示。



图 9-7　“隐藏桌面上‘网上邻居’图标”的策略设置

如果要隐藏桌面上的所有图标,只要启用“隐藏和禁用桌面上的所有项目”即可。当启用了“删除桌面上的‘我的文档’图标”和“删除桌面上的‘我的电脑’图标”两个选项以后,“我的电脑”和“我的文档”图标将从计算机桌面上消失;同样,如果要让“回收站”图标消失,只需启用“从桌面删除回收站”策略选项。

② 退出时不保存桌面设置(Windows 2000/XP/2003)

此策略可以防止用户保存对桌面的某些更改。如果启用这个策略,用户仍然可以对桌面做更改,但有些更改,如图标的位置、任务栏的位置及大小,在用户注销后都无法保存,不过任务栏上的快捷方式可以被保存。

在右侧窗格中启用“退出时不保存设置”策略选项,如图 9-8 所示。



图 9-8 "退出时不保存设置"的策略设置

③ 屏蔽"清理桌面向导"功能(Windows XP/2003)

"清理桌面向导"会每隔 60 天自动在用户的计算机上运行，以清除那些不经常使用或者从不使用的桌面图标。如果启用此策略设置，可以屏蔽"清理桌面向导"；如果禁用或不配置此设置，"清理桌面向导"会按照默认设置每隔 60 天运行一次。

打开右侧窗格中的"删除清理桌面向导"，根据需要设置策略选项，如图 9-9 所示。



图 9-9 "删除清理桌面向导"的策略设置

以上介绍了几个关于桌面的组策略配置项目，在"组策略控制台"→"用户配置"→"管理模板"→"桌面"下还有其他若干组策略配置项目，可根据需要来配置，这里不再赘述。

(2)"任务栏"和"开始"菜单设置

位置：组策略控制台→用户配置→管理模板→任务栏和开始菜单

① “开始”菜单设置

如果觉得 Windows 的“开始”菜单太臃肿，可以将不需要的菜单项从“开始”菜单中删除。例如，要从“开始”菜单中删除“我的文档”图标，启动相应的策略即可，如图 9-10 所示。

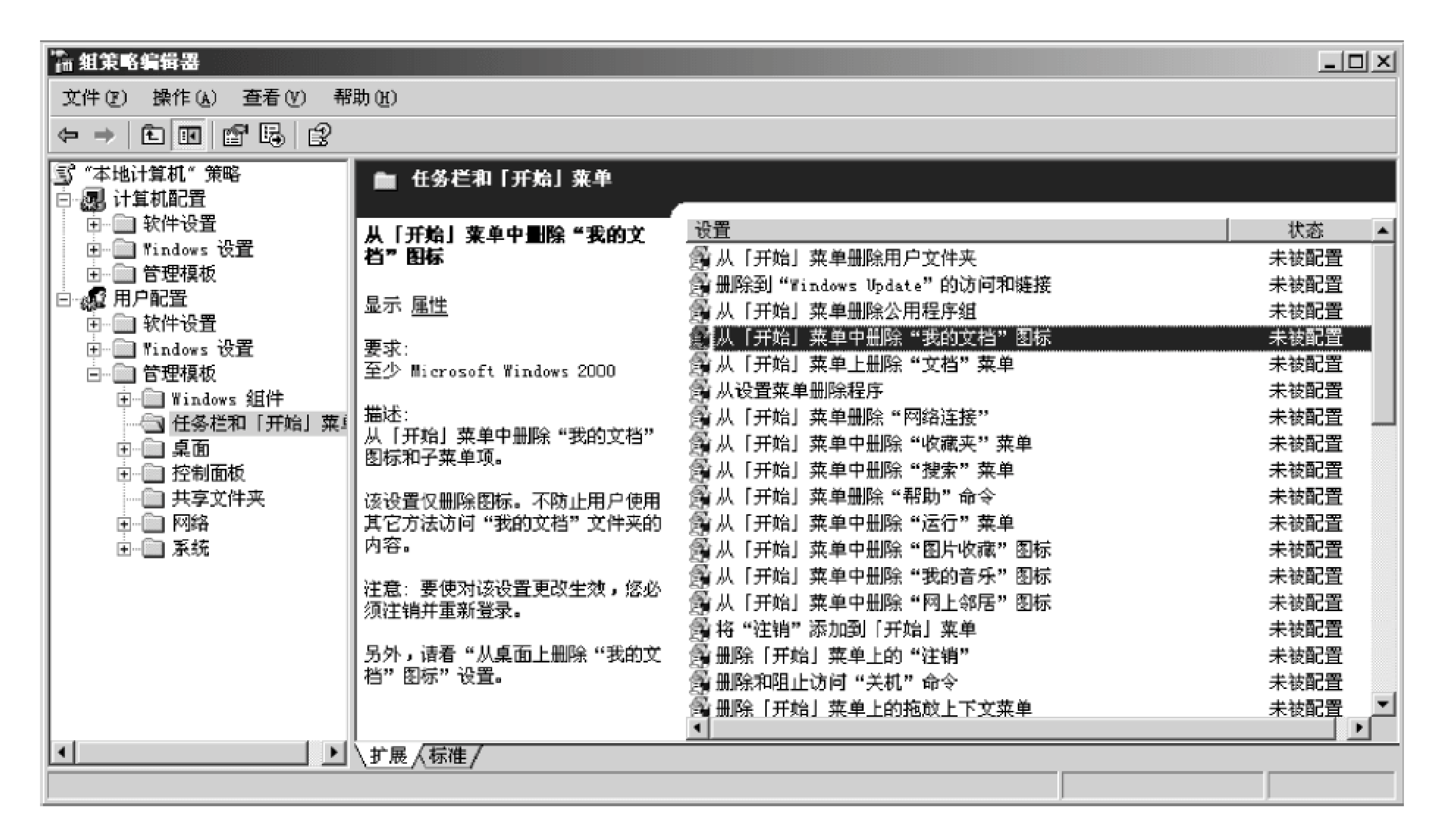


图 9-10　“从「开始」菜单中删除‘我的文档’图标”的策略设置

在组策略右侧窗格中，提供了“从「开始」菜单删除用户文件夹”、“删除到‘Windows Update’的访问和链接”、“从「开始」菜单删除公用程序组”、“从「开始」菜单中删除‘我的文档’图标”等多种组策略配置项目。只要将不需要的菜单项所对应的策略启用即可。

② “任务栏”和“开始”菜单设置

如果不想随意让他人更改“任务栏”和“开始”菜单的设置，只要将组策略控制台右侧窗格中的“阻止更改‘任务栏和「开始」菜单’设置”和“阻止访问任务栏的上下文菜单”两个策略项启用即可，如图 9-11 所示。



图 9-11　“阻止更改‘任务栏和「开始」菜单’设置”的策略设置

这样，当右击任务栏并单击“属性”时，系统会出现一个错误消息，且当右击任务栏及任务栏上的项目时，例如“开始”按钮、时钟和“任务栏”按钮，弹出菜单会隐藏。

③ 禁止“注销”和“关机”(Windows 2000/XP/2003)

当计算机启动以后，如果不希望这个用户再进行“关机”和“注销”操作，那么可将组策略控制台右侧窗格中的“删除开始菜单上的‘注销’”和“删除和阻止访问‘关机’命令”两个策略启用，如图 9-12 所示。

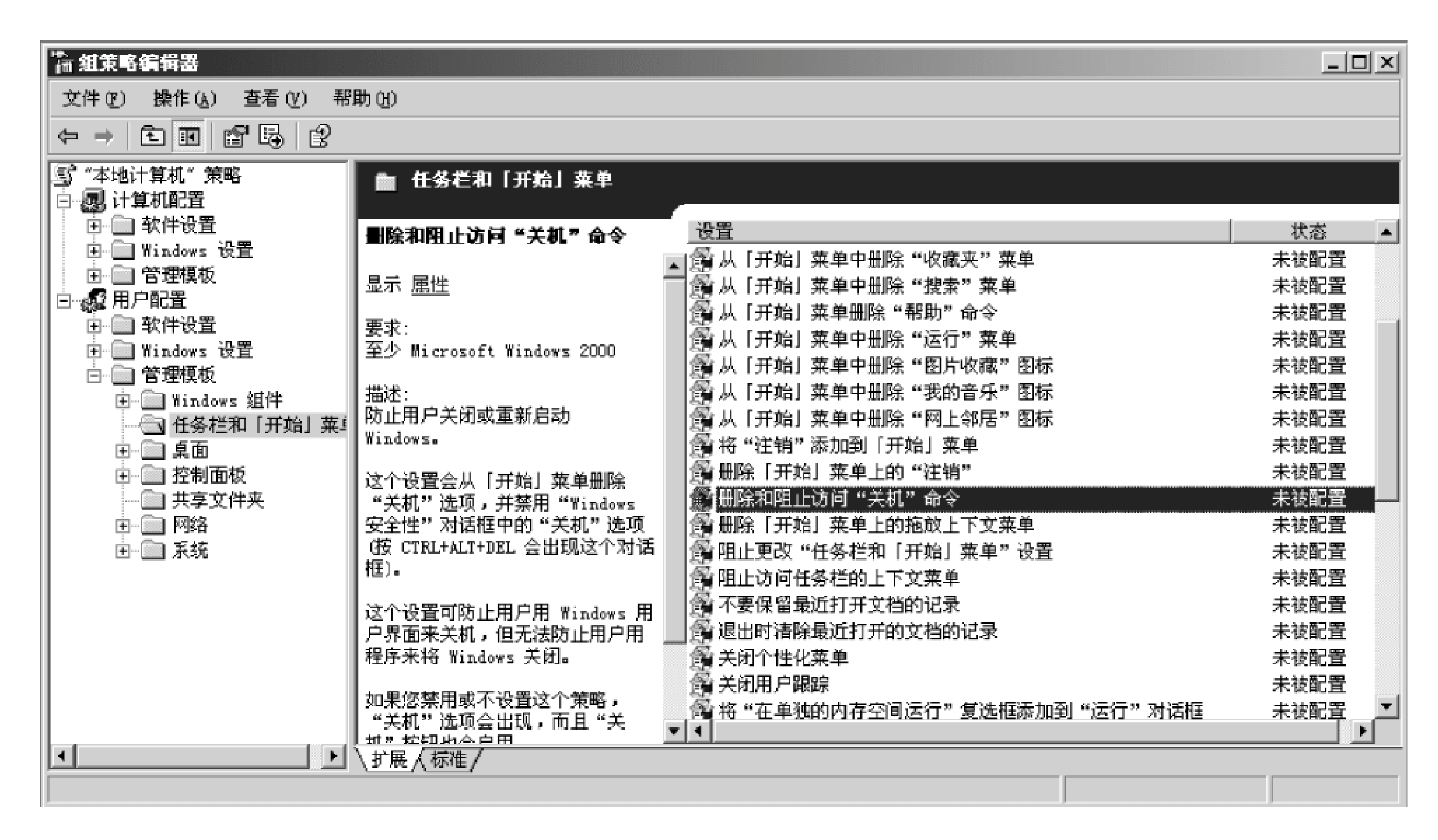


图 9-12 “删除和阻止访问‘关机’命令”的策略设置

这个设置会从“开始”菜单删除“关机”选项，并禁用“Windows 任务管理器”对话框，按 Ctrl+Alt+Delete 组合键，会出现这个对话框中的“关机”选项。此设置虽然可防止用户用 Windows 界面来关机，但无法防止用户用其他第三方工具程序关闭 Windows。

值得注意的是，如果启用了“删除开始菜单上的‘注销’”选项，会从“开始菜单选项”删除“显示注销”项目。用户无法将“注销<用户名>”项目还原到“开始”菜单，只能通过手动修改注册表的方法实现。这个设置只影响“开始”菜单，不影响 “Windows 任务管理器”对话框上的“注销”项目，因此需要同时启用“删除和阻止访问‘关机’命令”，并且不妨碍用户用其他方法注销。

④ 用组策略保护个人文档隐私(Windows 2000/XP/2003)

Windows 有个高级智能功能，记录用户曾经访问过的文件。虽然这个功能可以方便用户再次打开该文件，但出于安全和性能的考虑(例如，不想让人知道自己浏览过哪些网页和打开过哪些文件)，有时需要屏蔽此功能。利用组策略，只要在右侧窗格中启用“不要保留最近打开文档的记录”和“退出时清除最近打开的文档的记录”两个策略即可，如图 9-13 所示。

另外，如果启用此策略设置但不启用“从开始菜单中删除文档菜单”策略设置，“文档”菜单还会出现在“开始”菜单上，但是该菜单为空菜单。如果启用此策略设置，后来又禁用它并将它设置为“未配置”，则启用策略设置之前保存的文档快捷方式会重新出现在“文档”菜单和应用程序的“文件”菜单中。



图 9-13　"退出时清除最近打开的文档的记录"的策略设置

(3) IE 设置

微软的 Internet Explorer 让我们可以轻松地在互联网上遨游，但要想用好 Internet Explorer，必须将它配置好。在 IE 浏览器的"Internet 选项"窗口中提供了比较全面的设置选项，例如"首页"、"临时文件夹"、"安全级别"和"分级审查"等项目，但部分高级功能没有提供，通过组策略可轻松实现这些功能。

位置：组策略控制台→用户配置→管理模板→Windows 组件→Internet Explorer(需添加 inetres. adm 模板文件)

① 禁用"在新窗口中打开"菜单项

出于对安全的考虑，有时候有必要屏蔽 IE 的一些功能菜单。组策略提供了丰富的设置项目，比如禁用"另存为..."、"文件"、"新建"等。下面以"禁用'在新窗口中打开'菜单项"为例介绍具体的设置方法。

打开"组策略控制台"→"用户配置"→"管理模板"→"Windows 组件"→"Internet Explorer"→"浏览器菜单"，然后打开"禁用'在新窗口中打开'菜单项"并设置为"启用"，如图 9-14 所示。

启用该策略后，用户在某个链接上右击，然后单击"在新窗口中打开"时，该命令将不起作用。该策略可与"'文件'菜单：禁用'新建'菜单项"一起使用，后者禁止用户通过单击"文件"菜单指向"新建"，然后单击"窗口"在新窗口中打开浏览器。

注意：启用该策略后，单击"在新窗口中打开"命令，将无法在新窗口中打开链接，系统会提示用户该命令无效，网页自动打开的窗口也全部被禁止，也达到了屏蔽弹出广告窗口的效果。

② 限制 IE 浏览器的保存功能

在使用 IE 浏览网页的过程中，当遇到好的图片、文章等资源时，可以使用"另存为"功能将它保存到本地硬盘中。当多人共用一台计算机时，为了保持硬盘的整洁，需要对浏览器的



图 9-14 "禁用'在新窗口中打开'菜单项"的策略设置

保存功能进行限制。那么如何才能实现呢?可以这样操作:打开"组策略控制台"→"用户配置"→"管理模板"→"Windows 组件"→"Internet Explorer"→"浏览器菜单",然后将右侧窗格中的"'文件'菜单:禁用'另存为...'菜单项"、"'文件'菜单:禁用另存为'网页,全部'格式"、"'查看'菜单:禁用'源文件'菜单项"和"禁用上下文菜单"等策略项目全部启用,如图 9-15 所示。

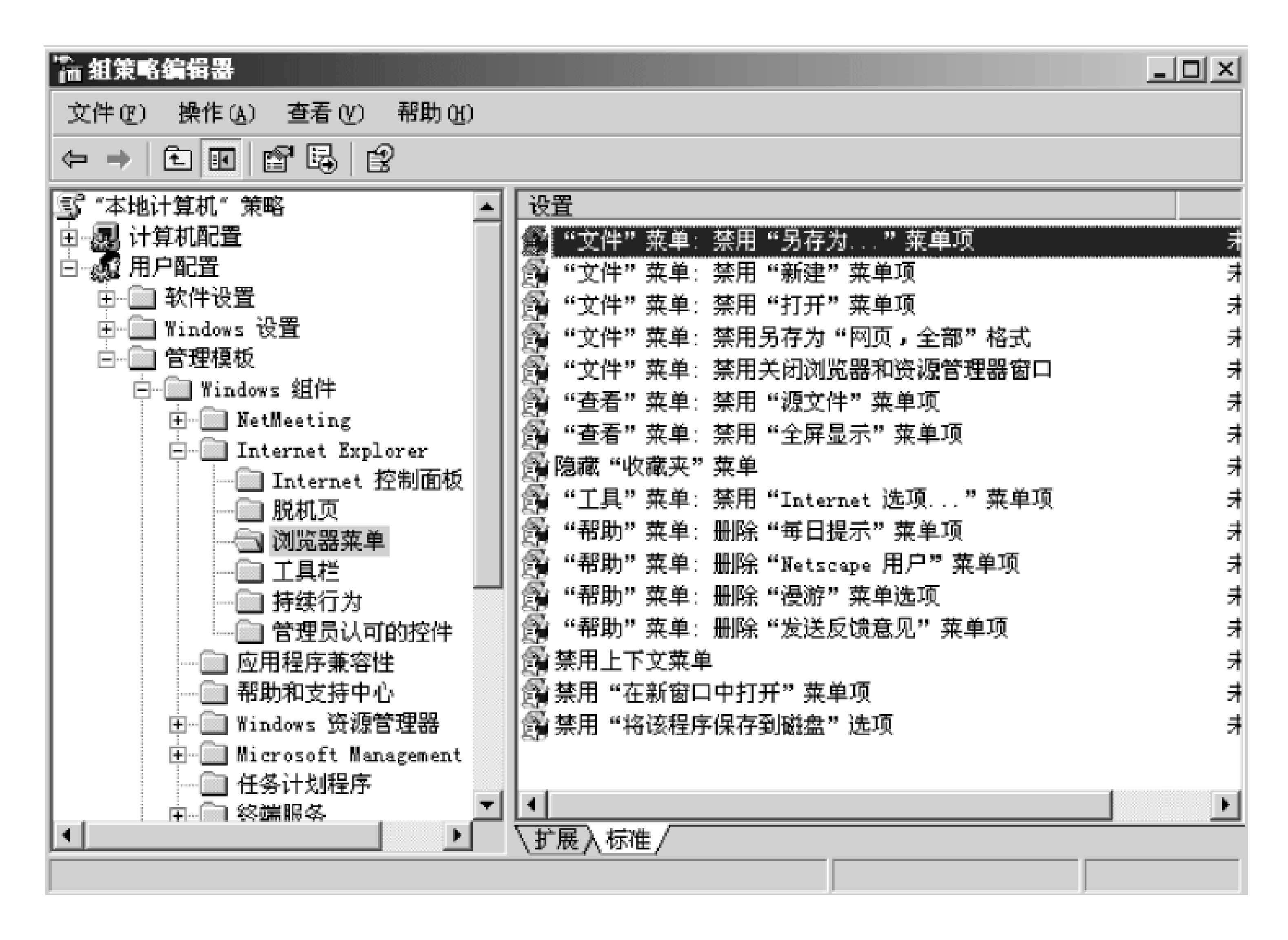


图 9-15 "'文件'菜单:禁用'另存为...'菜单项"的策略设置

如果不希望别人对 IE 浏览器的设置随意更改,可以将"'工具'菜单:禁用'Internet 选项...'菜单项"策略启用。另外,根据个人的需要,在该窗格中还可以禁用其他项目。

③ 禁用"Internet 选项"控制面板

上面提到了"禁用 Internet 选项"的功能,使用该功能可以达到阻止别人对 IE 浏览器随便设置的目的。而这种方法无法具体禁用 Internet 选项中的控制模板项目,因此给具体应

用带来麻烦。通过下面的组策略设置方法，可以实现这一要求。

打开“组策略控制台”→“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“Internet 控制面板”，在右边窗格中可以看到“禁用常规页”、“禁用安全页”等组策略项目。下面以“禁用常规页”为例来说明。

打开右边窗格中的“禁用常规页”并设置为“启用”，如图 9-16 所示。



图 9-16　“禁用常规页”的策略设置

当再次打开“Internet 选项控制”面板时，会发现“常规”项目已经没有了，用户将无法看到和更改主页、缓存、历史记录、网页外观以及辅助功能的设置，因为该策略将删除界面上的“常规”选项卡。所以，如果设置了该策略，则无须设置位于“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”中的诸如“禁用更改主页设置”、“禁用更改颜色设置”等策略。

④ 禁止修改 IE 浏览器的主页

如果不希望他人对自己设定的 IE 浏览器主页随意更改，可以打开“组策略控制台”→“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“工具栏”，然后选择“禁用更改主页设置”组策略并启用。另外，在这个窗格中还提供了“更改历史记录设置”、“更改颜色设置”和“更改 Internet 临时文件设置”等项目的禁用功能。

启用此策略后，在 IE 浏览器的“Internet 选项”对话框中，其“常规”选项卡的“主页”区域的设置将变灰。

注意：如果设置了位于“组策略控制台”→“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“Internet Explorer 控制面板”中的“禁用常规页”策略，则无须设置该策略，因为“禁用常规页”策略将删除界面上的“常规”选项卡。

⑤ 自定义 IE 工具栏

IE 工具栏的背景和上面的按钮都是可以自定义的，以前大多采用手动修改注册表的方法，不过并不直观，现在可以用组策略更方便地达到效果，打造属于用户自己的 IE 浏览器。

打开“组策略控制台”→“用户配置”→“Windows 设置”→“Internet Explorer 维护”→“浏览器用户界面”下的“浏览器工具栏自定义”策略配置项目，如图 9-17 所示。

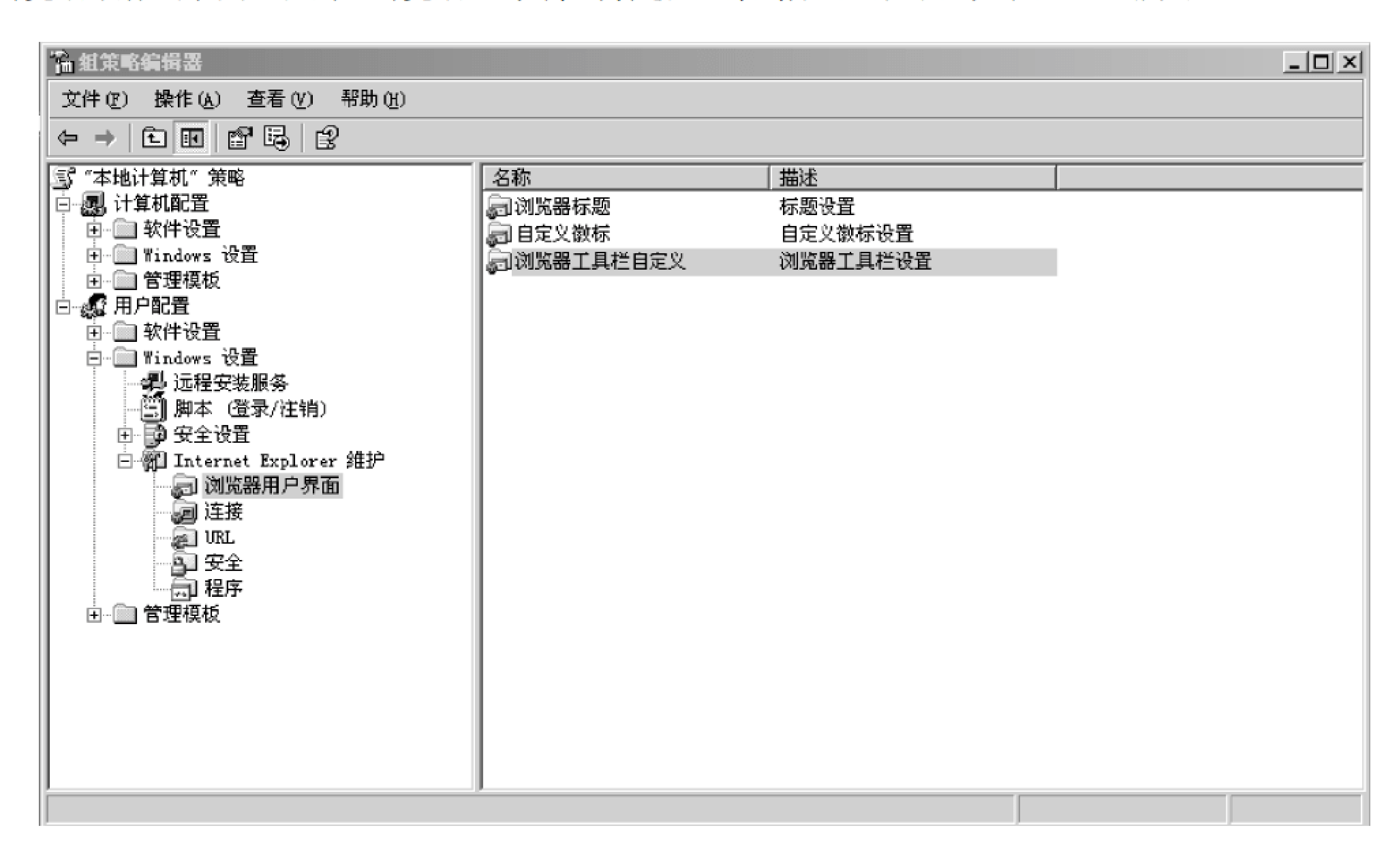


图 9-17 “浏览器工具栏自定义”的策略设置

在这里，可以自定义浏览器工具栏的背景图片。单击“浏览”按钮，然后选择一个 BMP 的位图文件，如图 9-18 所示。

图 9-18 “浏览器工具栏自定义”对话框

注意：工具栏背景应该与工具栏大小相同，亮度应该足以显示黑色文字，否则实际效果并不理想。

接下来，在 IE 的工具栏上添加快捷方式，比如添加“我的 QQ”，操作步骤为：单击“添加”按钮，在“工具栏标题”中输入“我的 QQ”；再在“工具栏操作”中选择 QQ 程序的路径；最后选择“颜色图标”和“灰度图标”的路径。设置完成后单击“确定”按钮，再次打开 IE 浏览器，就可以看到修改的效果。

(4) Windows 高级功能设置

① 在 Windows XP/2003 中实现远程关机

在 Windows XP/2003 中，新增了一条命令行工具“shutdown”，它可以关闭或重新启动本地或远程计算机。利用它不但可以注销用户、关闭或重启计算机，还可以实现定时关机、远程关机。该命令的语法格式如图 9-19 所示。



图 9-19　“shutdown”命令使用帮助

下面是该命令的一些基本用法。

- 注销当前用户：

```
shutdown -l
```

该命令只能注销本机用户，对远程计算机不适用。

- 关闭本地计算机：

```
shutdown -s
```

- 重启本地计算机：

```
shutdown -r
```

- 定时关机：

```
shutdown -s -t 30
```

指定在 30s 之后自动关闭计算机。

- 中止计算机的关闭：有时用户设定了计算机定时关机后，如果出于某种原因想取消这次关机操作，可以用 shutdown - a 来中止。

- 使用图形界面设置关机：shutdown 命令也可以用图形界面来设置。在命令行窗口输入“shutdown -i”，然后按“Enter”键，将弹出“远程关机对话框”，如图 9-20 所示，可以根据需要进行设置。

图 9-20 “远程关机对话框”设置

在该命令的格式中，有一个参数[-m [\\ComputerName]，用于指定将要关闭或重启的计算机名称；若省略，则默认为对本机操作。

例如，在 30s 内关闭局域网内一台同样装有 Windows XP 或 Windows 2003 系统的计算机，计算机名为 melody，使用如下命令：

```
shutdown -s -m \\melody -t 30
```

如果该命令执行后，计算机 melody 一点反应都没有，屏幕上却提示“Access is denied（拒绝访问）”，其原因是在 Windows XP 默认的安全策略中，只有管理员组的用户才有权从远端关闭计算机，一般情况下从局域网内的其他计算机访问该计算机时只有 guest 用户权限，所以当执行上述命令时，会出现“拒绝访问”的情况。利用组策略，可赋予 guest 用户远程关机的权限。

打开“组策略控制台”→“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”→“从远程系统强制关机”，如图 9-21 所示。在弹出的对话框中显示目前只有“Administrators”组的成员才有权从远程关机。单击对话框下方的“添加用户或组”按钮，然后在新弹出的对话框中输入“guest”，再单击“确定”按钮。通过上述操作，便给计算机 melody 的 guest 用户授予了远程关机的权限。

以后，倘若要远程关闭计算机 melody，只要在网络中其他装有 Windows XP/2003 的计算机中输入命令“shutdown -s -m \\melody -t 60”即可。这时，在 melody 计算机的屏幕上将显示“系统关机”的对话框；在对话框下方还有一个计时器，显示离关机还有多少时间。在等待关机的时间里，用户可以执行其他任务，如关闭程序、打开文件等，但无法关闭该对话

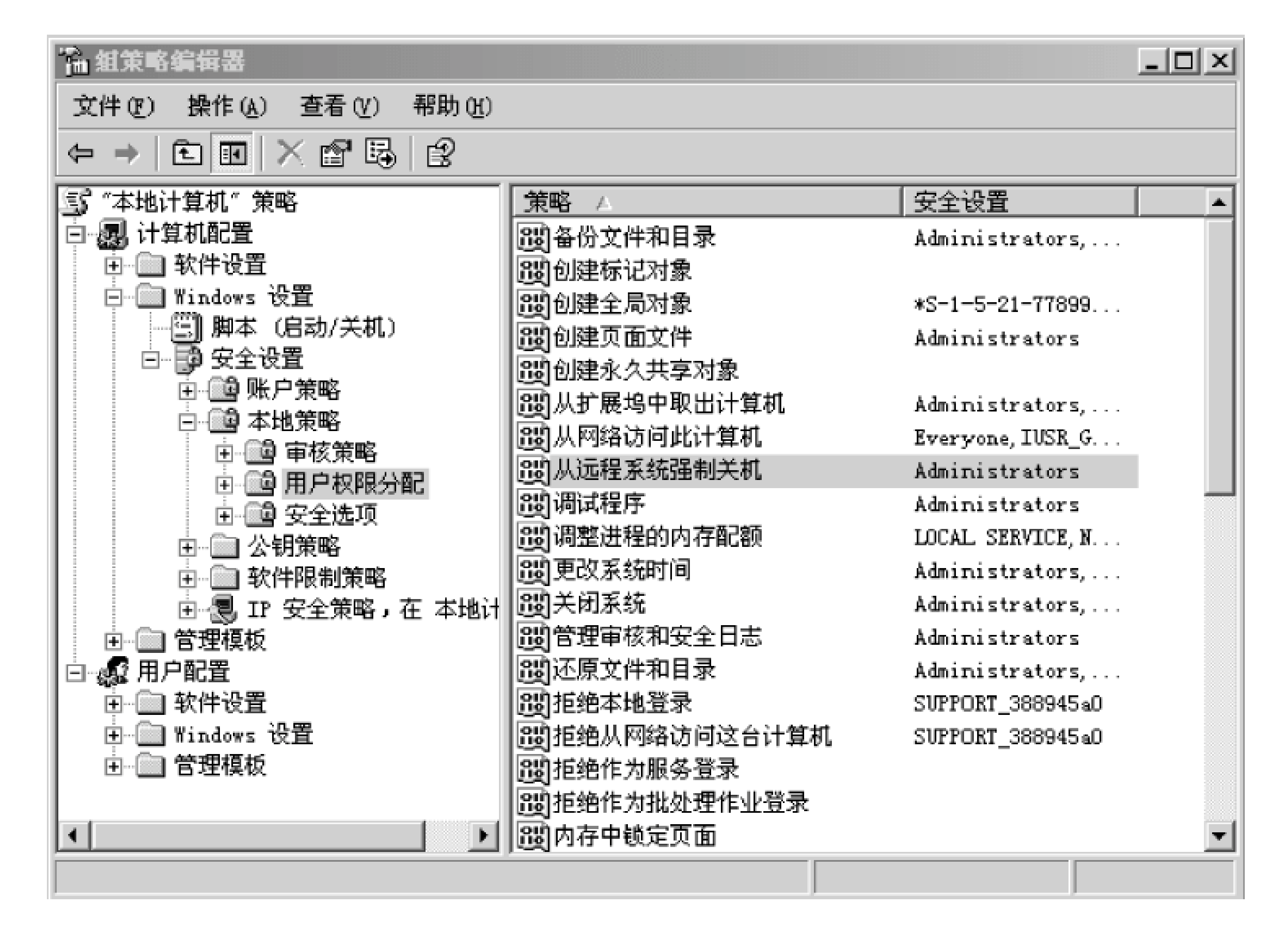


图 9-21　“从远程系统强制关机”的策略设置

框，除非用 shutdown -a 命令来中止关机任务。

② 隐藏“我的电脑”中指定的驱动器

此组策略可以从“我的电脑”和“Windows 资源管理器”上删除代表所选硬件驱动器的图标，并且驱动器号代表的所有驱动器不出现在标准的打开对话框上。

打开“组策略控制台”→“用户配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”中的“隐藏‘我的电脑’中的这些指定的驱动器”并启用此策略，如图 9-22 所示。



图 9-22　“隐藏‘我的电脑’中的这些指定的驱动器”的策略设置

弹出“隐藏‘我的电脑’中的这些指定的驱动器 属性”对话框，在其下面的列表框中选择一个驱动器或几个驱动器进行隐藏设置，如图 9-23 所示。



图 9-23　“隐藏‘我的电脑’中的这些指定的驱动器 属性”对话框

注意：这项策略只删除驱动器图标，用户仍可通过其他方式继续访问驱动器的内容。同时，这项策略不会防止用户使用程序访问这些驱动器或其内容，也不会防止用户使用磁盘管理即插即用来查看并更改驱动器特性。

③ 防止从“我的电脑”访问驱动器

此策略让用户无法查看在“我的电脑”或“Windows 资源管理器”中所选驱动器的内容。同时，禁止使用运行对话框、镜像网络驱动器对话框或 Dir 命令查看在这些驱动器上的目录。

打开“组策略控制台”→“用户配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”中的“防止从‘我的电脑’访问驱动器”并启用此策略，如图 9-24 所示。

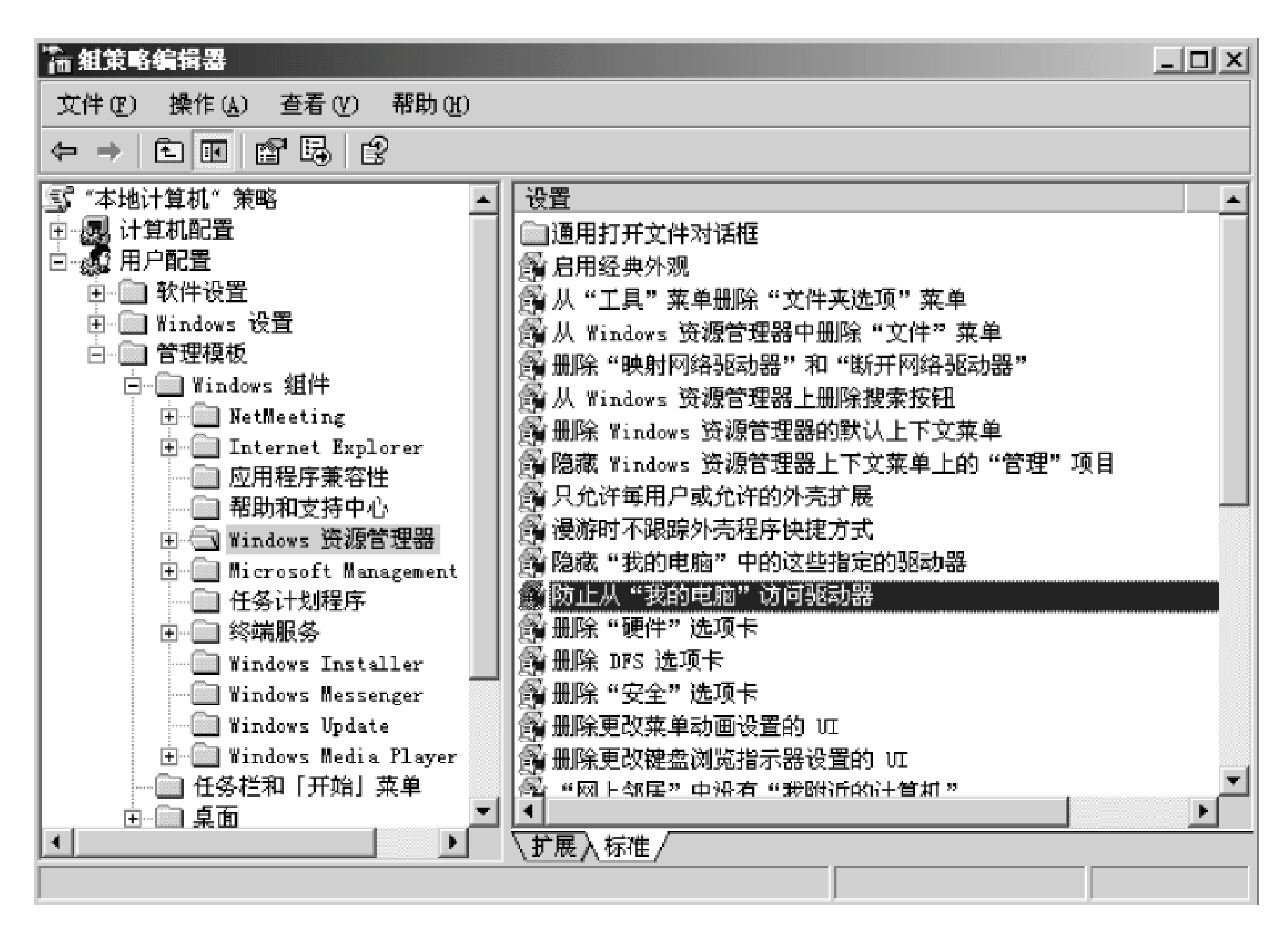


图 9-24　“防止从‘我的电脑’访问驱动器”的策略设置

此时，会弹出“隐藏‘我的电脑’中的这些指定的驱动器 属性”对话框，在其下面的列表框中选择一个驱动器或几个驱动器进行隐藏设置。注意，这些代表指定驱动器的图标仍旧会出现在“我的电脑”中，如果用户双击图标，会出现一条消息，解释设置防止这一操作。同时，这些设置不会防止用户使用其他程序访问本地和网络驱动器，并且不防止使用磁盘管理即插即用查看和更改驱动器特性。

④ 禁止使用文件夹选项

在 Windows 操作系统中，“文件夹选项”是比较常用的功能之一。使用“文件夹选项”功能，用户可以查看隐藏在计算机中的文件、设置文件夹窗口的打开方式以及其他许多有关文件夹选项的设置。如果用户不希望其他用户更改自己在计算机中的各项设置，可以将该功能禁用。

打开“组策略”窗口，然后在左边窗格中依次展开“用户配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”，可以在右边窗格中看到“从‘工具’菜单删除‘文件夹选项’菜单”，如图 9-25 所示。

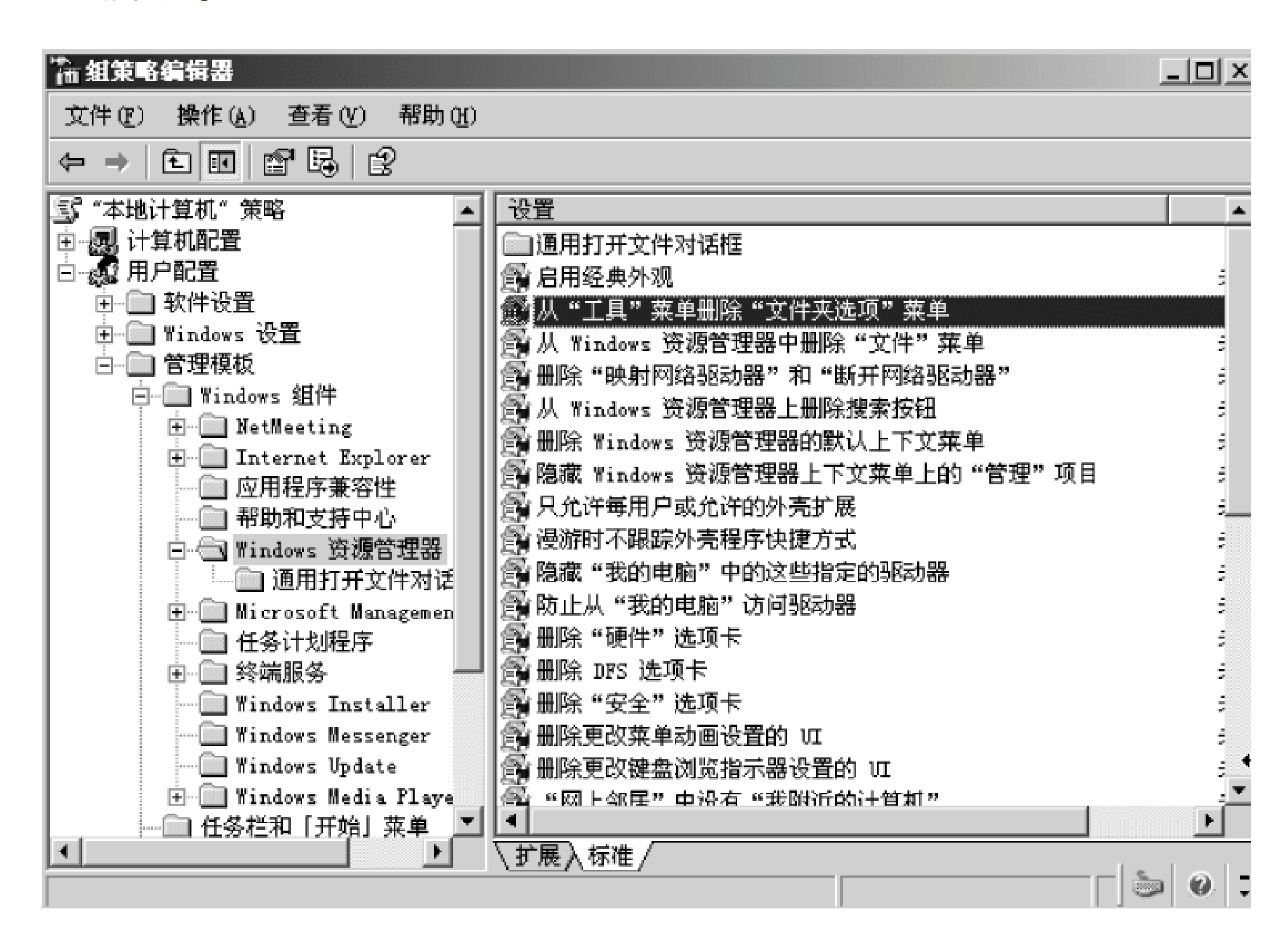


图 9-25　“从‘工具’菜单删除‘文件夹选项’菜单”的策略设置

在其上右击，从弹出的快捷菜单中选择“属性”菜单项，或者直接双击它，打开对话框。选择“已启用”单选按钮，然后单击“确定”按钮。当用户再在窗口中选择“工具”菜单项时，会发现里面已经没有了“文件夹选项”菜单项。如果用户想要重新使用“文件夹选项”功能，可以进入“组策略”窗口中的相同目录，找到“从‘工具’菜单删除‘文件夹选项’菜单”选项并双击，然后在其属性对话框将“从‘工具’菜单删除‘文件夹选项’菜单”选项设置为“未配置”或者“已禁用”。

⑤ 防止访问控制面板

控制面板是 Windows 中最重要的组件之一。要在组策略中设置禁止访问控制面板，具体的操作步骤如下：

打开“组策略”窗口，然后在左边窗格中依次展开“用户配置”→“管理模板”→“控制面板”，用户可以在右边窗格中看到“禁止访问控制面板”选项，如图 9-26 所示。

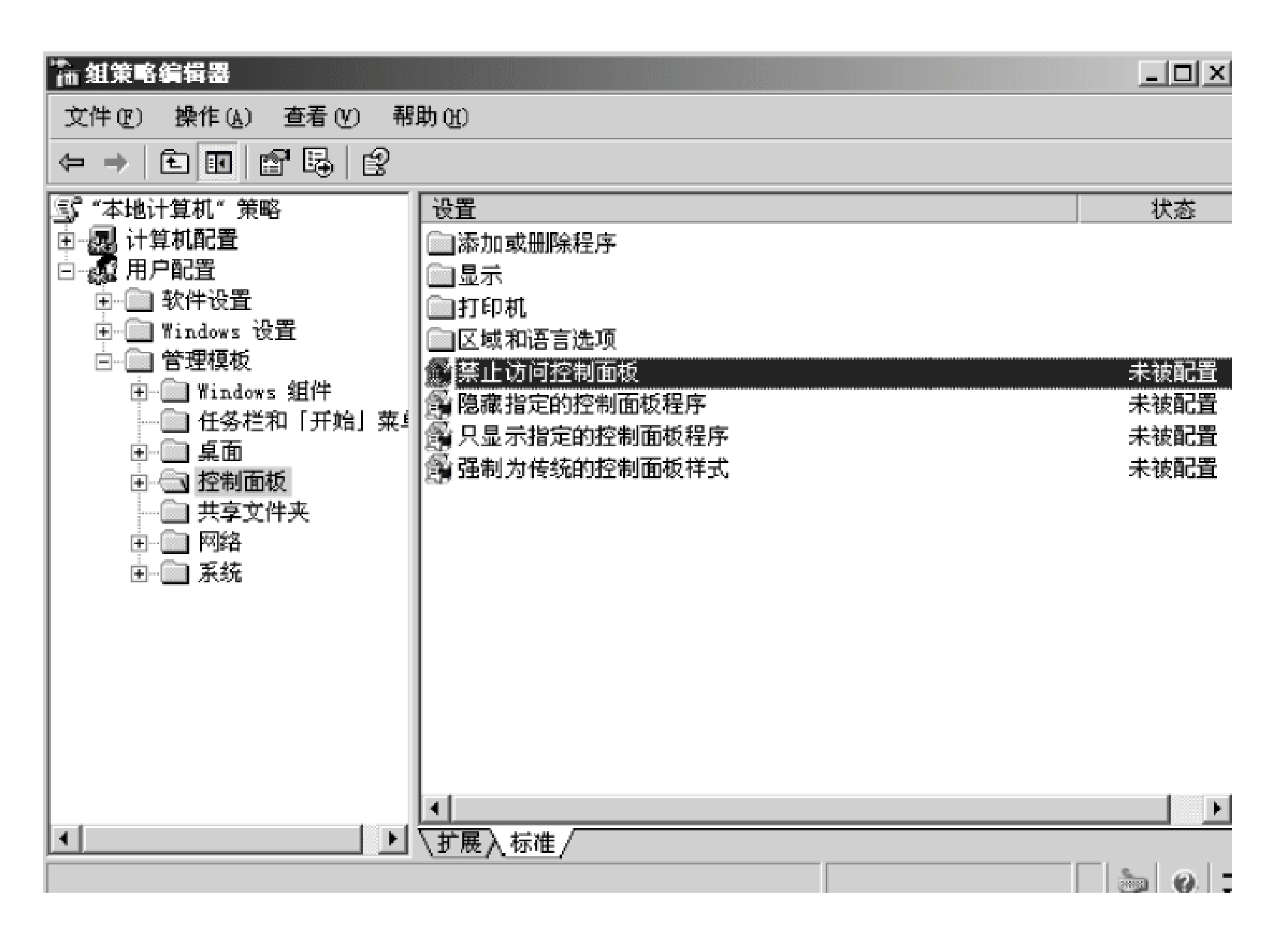


图 9-26 “禁止访问控制面板”的策略设置

在其上右击,从弹出的快捷菜单中选择“属性”菜单项,或者直接双击它,打开对话框。选择“已启用”单选按钮,然后单击“应用”和“确定”按钮。这样,当用户再次打开“开始”菜单时,会发现其中已经没有了“控制面板”菜单项。如果用户想要重新使用控制面板,在上述操作的同一目录下,将“禁止访问控制面板”选项设置为“未配置”或者“已禁用”即可。

⑥ 禁用“添加/删除程序”(Windows 2000/XP/2003)

“控制面板”中的“添加或删除程序”项目允许安装、卸载、修复并添加或删除 Windows 的功能和组件及很多种类的 Windows 程序。如果想阻止其他用户安装或卸载程序,可利用组策略来实现。

打开“组策略控制台”→“用户配置”→“管理模板”→“控制面板”→“添加”→“删除程序”中的“删除‘添加/删除程序’程序”并启用此策略,当再次打开“控制面板”中的“添加/删除程序”模块时,会自动弹出警告窗口,而“添加/删除程序”无法运行。

此外,在“添加/删除程序”分支中还可以对 Windows“添加/删除程序”项中的“添加新程序”、“从 CD-ROM 或软盘添加程序”、“从 Microsoft 添加程序”、“从网络添加程序”等项进行隐藏。通过设置这些策略项目,来保护计算机中的系统文件及应用程序。

⑦ 禁止使用命令提示符(Windows 2000/XP/2003)

在 Windows 2000/XP/2003 下,可以运行 cmd. exe 进入命令提示符状态,并可以继续运行一些 DOS 命令和其他命令行程序。出于对安全的考虑,有些系统应该屏蔽此功能。

打开“组策略控制台”→“用户配置”→“管理模板”→“系统”中的“阻止访问命令提示符”并启用此策略,并在下面的列表框中选择是否“也停用命令提示符脚本处理”。这个设置还决定批处理文件 . cmd 和. bat 是否可以在计算机上运行。

如果启用这个设置,在用户试图打开命令窗口时,系统会显示一条消息,解释设置阻止这一操作。

⑧ 禁止注册表编辑器

打开“组策略”窗口,然后在左边窗格中依次展开“用户配置”→“管理模板”→“系统”,用户可以在右边窗格中看到“阻止访问注册表编辑工具”,如图 9-27 所示。

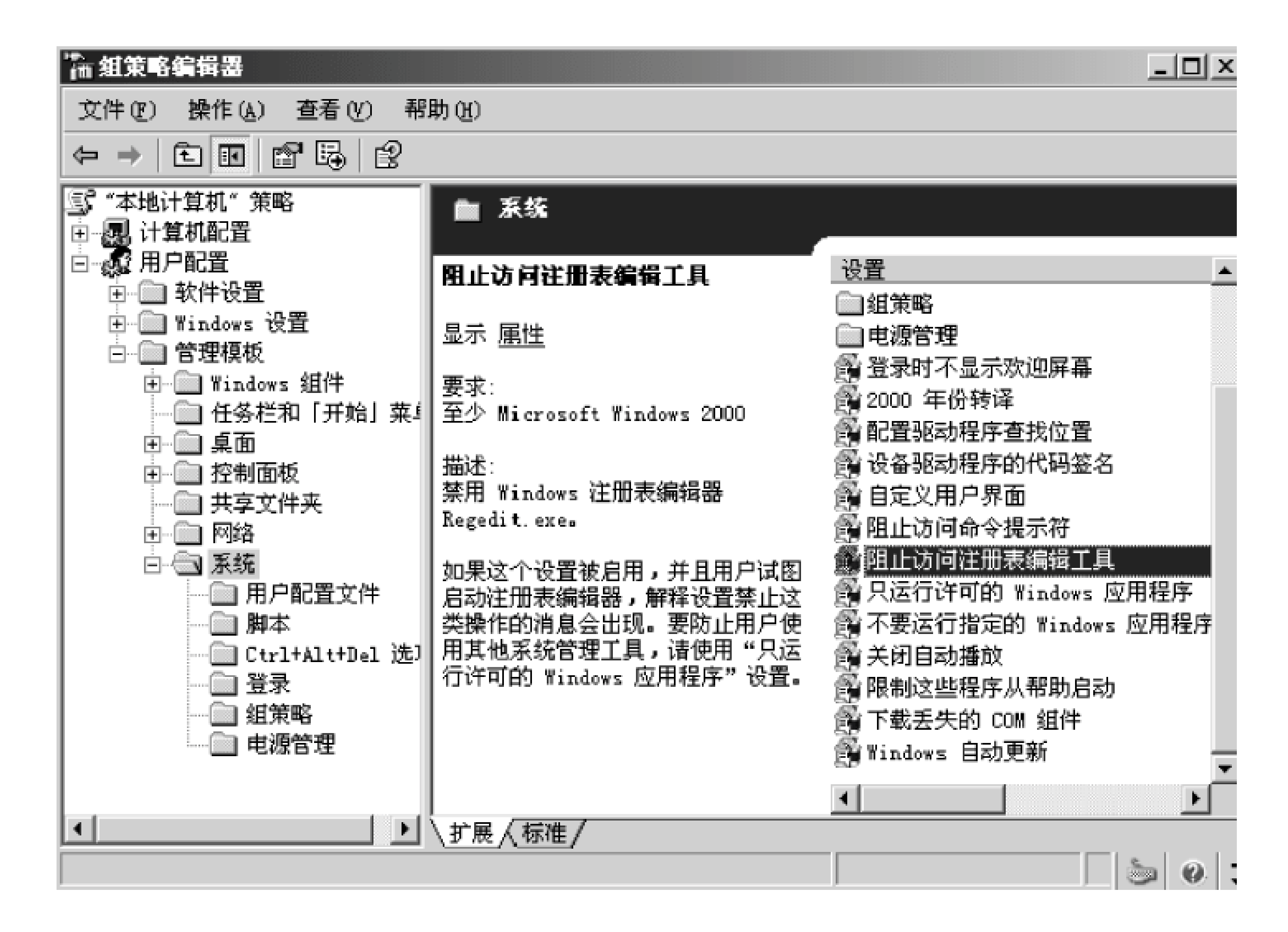


图 9-27　"阻止访问注册表编辑工具"的策略设置

在其上右击，从弹出的快捷菜单中选择"属性"菜单项，或者直接双击它，打开对话框。选择"已启用"单选按钮，然后单击"确定"按钮。此时下面的"禁用后台运行 regedit?"下拉列表被激活，用户可以从中选择"是"或"否"来决定是否禁用后台运行"regedit"命令。当用户再在运行中输入"regedit"命令时，会提示"注册编辑已被管理员停用"。

⑨ 限制可以使用的应用程序

有时用户所使用的计算机并非一人专用，而是多个人共用的，而且这些使用者的权限不一样，有的是管理员账户，有的是标准账户，有的则使用 Guest 账户。此时，管理员用户可以为其他用户设置可以使用的应用程序的限制，具体操作步骤如下。

打开"组策略"窗口，然后在左边窗格中依次展开"用户配置"→"管理模板"→"系统"，用户可以在右边窗格中看到"只运行许可的 Windows 应用程序"，如图 9-28 所示。

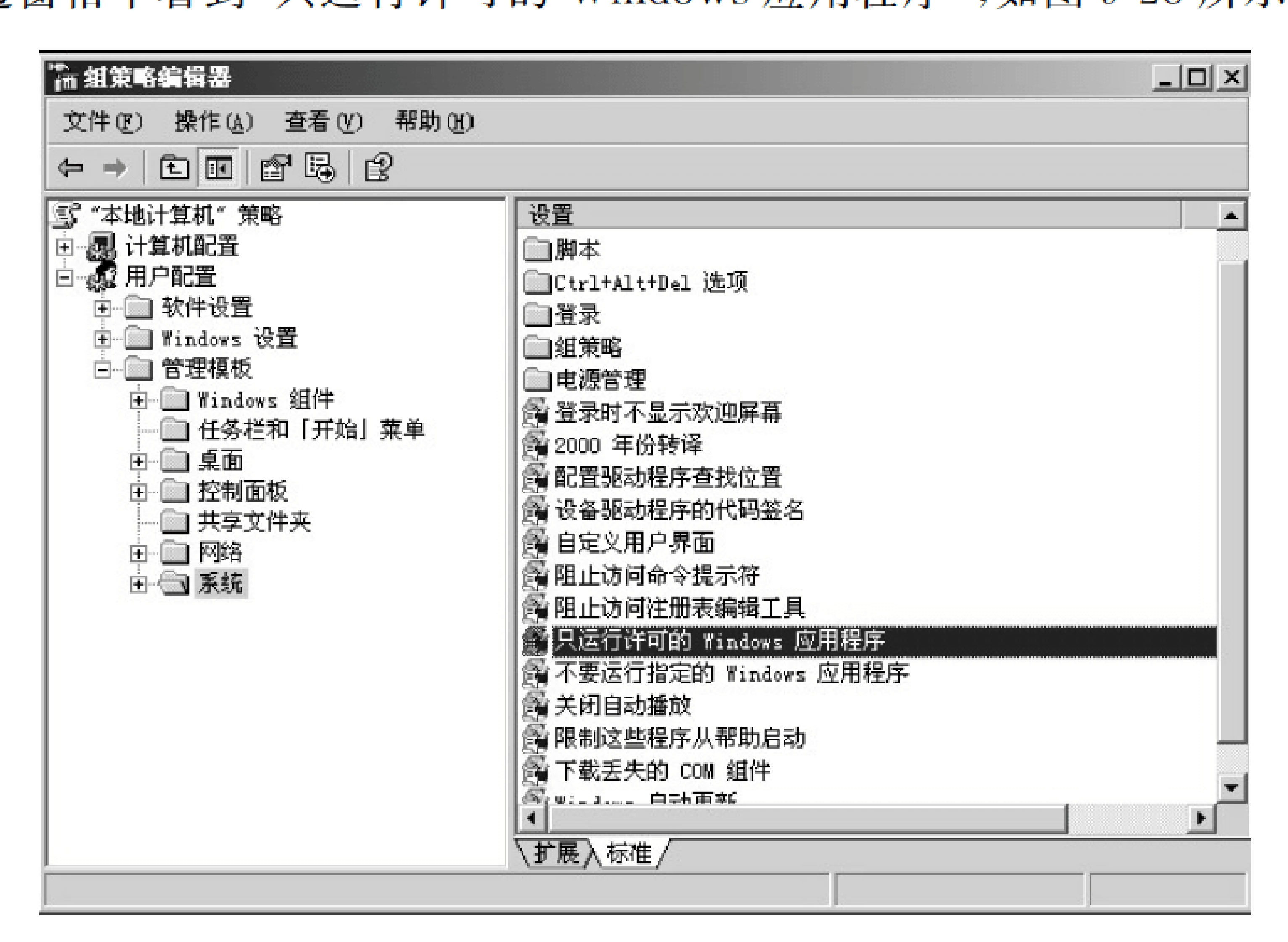


图 9-28　"只运行许可的 Windows 应用程序"的策略设置

在其上右击，从弹出的快捷菜单中选择“属性”菜单项，或者直接双击它，打开对话框。选择“已启用”单选按钮，下面的“允许的应用程序列表”右边的显示按钮被激活。单击“添加”按钮，输入想要设置为允许运行的应用程序，然后单击“确定”按钮。

另外，用户可以在右边窗格中找到“不要运行指定的 Windows 应用程序”选项，如图 9-29 所示。



图 9-29 “不要运行指定的 Windows 应用程序”的策略设置

双击打开其属性对话框，然后选择“已启用”单选按钮，下面的“不允许的应用程序列表”右边的显示按钮被激活。单击“添加”按钮，输入想要设置为不允许运行的应用程序，然后单击“确定”按钮。例如输入“notepad.exe”，设置“记事本”为不允许运行的应用程序。

9.4.3 任务 3：系统的安全管理

1. 任务目标

安全是计算机用户不能忽视的一个方面。设置完善的安全策略对于维护计算机系统的安全是很重要的。系统安全至关重要，它不仅影响着计算机能否处于一个稳定且安全、可靠的环境中，而且直接影响着用户的利益能否得到有效的保障。一些网络攻击者常常会利用用户计算机中的漏洞进行窃取和破坏活动，给用户带来不必要的损失。在与本地安全策略有关的策略选项中，有一些是与系统安全紧密相关的，对这些策略选项进行适当的设置，能够更好地维护计算机系统的安全。

2. 工作任务

（1）禁止在登录前关机；

（2）不显示上次登录的用户名。

3. 工作环境

一台预装 Windows Server 2003/XP 的主机。

4. 实施过程

(1) 禁止在登录前关机

此策略选项用来确定是否无须登录到系统便可关闭计算机。启用此策略时，在Windows 登录屏幕上的关机命令可用；禁用此策略时，用户必须能够成功登录到计算机并具有关闭系统的权限，才能够执行系统关闭操作。具体的操作步骤如下：

选择“开始”→“运行”菜单，打开“运行”对话框，然后输入“secpol.msc”命令，按“Enter”键打开“本地安全设置”窗口，再在左边窗格中依次展开“安全设置”→“本地策略”→“安全选项”，在右边窗格中找到“关机：允许系统在未登录前关机”选项，如图 9-30 所示。

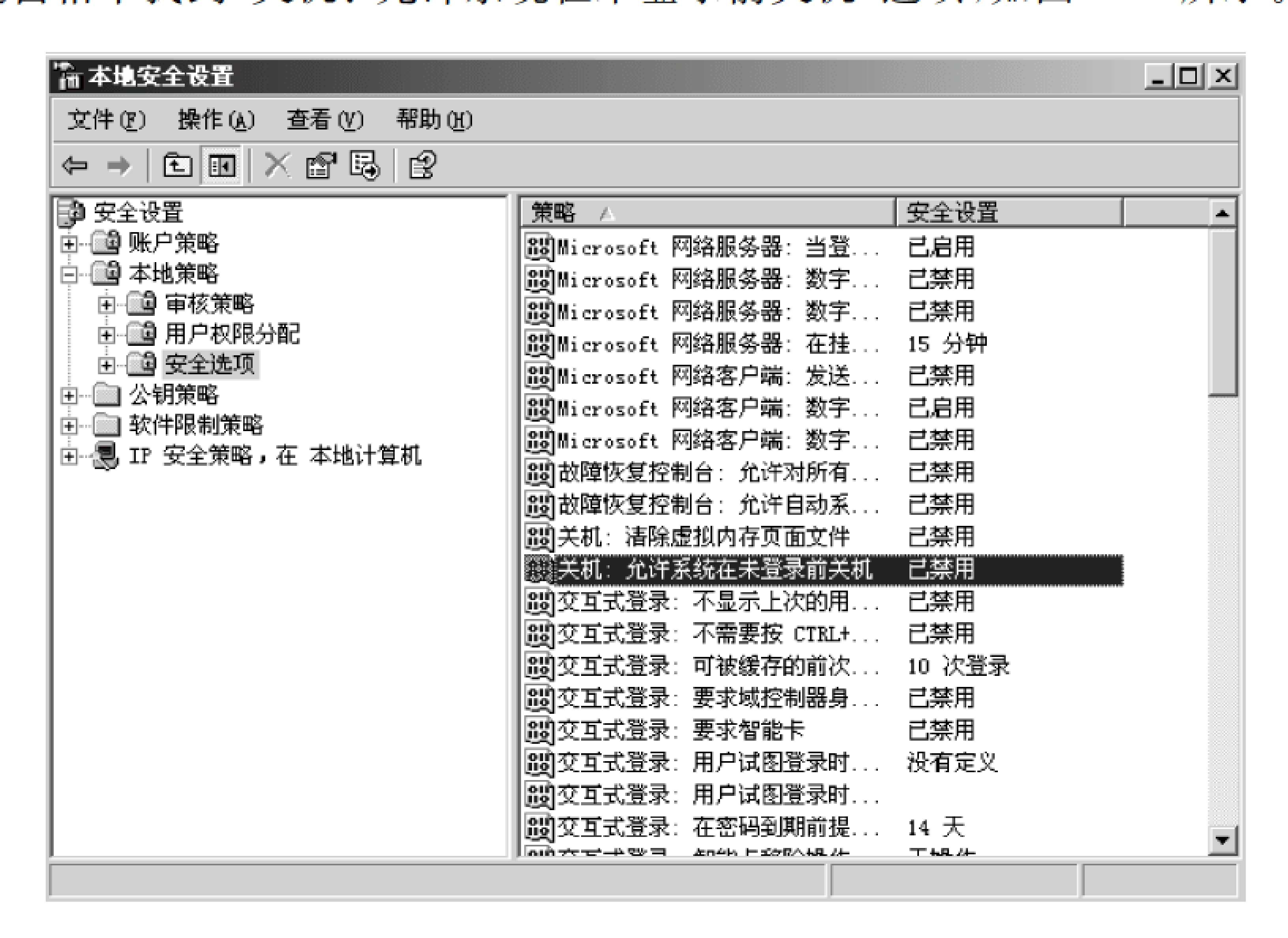


图 9-30　“关机：允许系统在未登录前关机”的策略设置

双击打开“属性”对话框，选择“已启用”单选按钮，然后单击“应用”和“确认”按钮。通常情况下，作为服务器的计算机是否能够保证运行正常、不受到恶意攻击和不中途断电关机等，对于局域网甚至是整个互联网都起着至关重要的作用，因此应该将该策略选项设置为“已禁用”。对于作为终端的计算机来说，不需要保证计算机一直处于开机状态，如果用户在登录界面以后不想使用计算机了，在登录界面上有一个“关机”选项显得方便很多。

(2) 不显示上次登录的用户名

该策略选项用来确定是否将上次登录到系统中的用户名显示在 Windows 登录界面中。很多情况下，这一功能的设置方便了用户登录系统，但另一方面为非法用户侵犯用户隐私带来了便利。如果启用该策略选项，则上次成功登录的用户的名称将不显示在登录界面中；如果禁用该策略选项，在 Windows 登录界面中会显示上次登录的用户名。具体的操作步骤如下：

① 打开“本地安全设置”窗口。

② 在左边窗格中依次展开“安全设置”→“本地策略”→“安全选项”。

③ 在右边窗格中找到“交互式登录：不显示上次的用户名”选项，如图 9-31 所示。

④ 双击打开其“属性”对话框，选择“已启用”单选按钮，然后单击“应用”和“确认”按钮。

注意：当启用了该策略选项之后，用户再次登录系统时，需要输入用户名和密码。

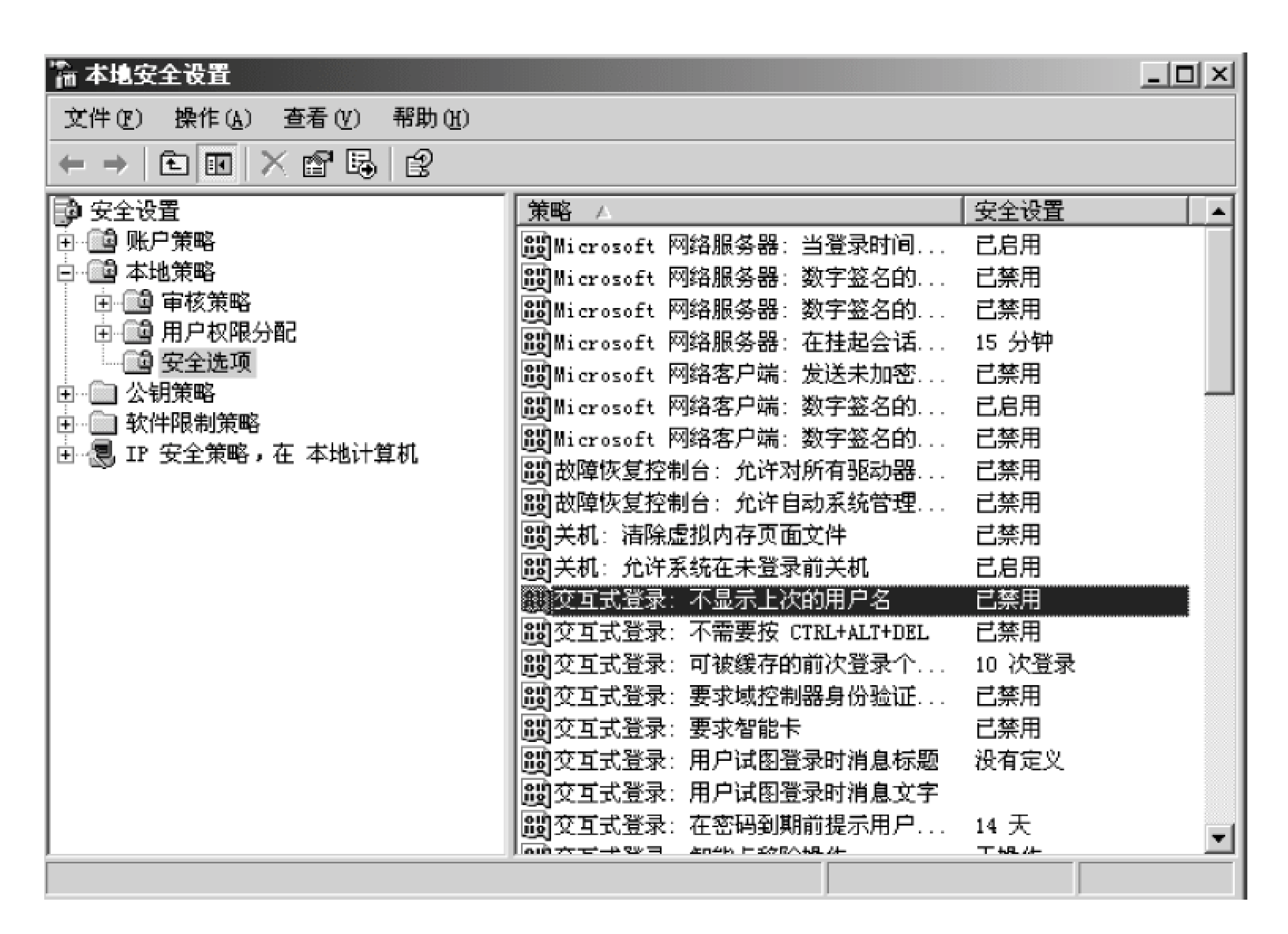


图 9-31 “交互式登录：不显示上次的用户名”的策略设置

9.5 常见问题解答

Windows 允许匿名用户执行某些操作，比如列举域账户和网络共享名。例如，当用户要给一个不需要维护互相信任关系的信任域中的用户进行访问授权时，这是非常方便的。默认情况下，匿名用户具有与授予给 everyone 组中的用户访问特定资源相同的访问权限。

9.6 过关练习

一、选择题

若在 Windows“运行”窗口中输入(   )命令，可运行 Microsoft 管理控制台。

A. cmd　　B. mmc　　C. autoexe　　D. tty

二、简答题

1. 如何利用组策略设置“不允许 SAM 账户匿名枚举”？
2. 如何利用组策略设置用户权限？

工作任务十

数据加密技术的使用

10.1 用户需求与分析

实际工作中,企业人员经常要利用互联网将一些重要文档传送给自己的客户或企业总部,但是互联网上存在很多不安全因素,如何对重要文档进行机密性保护是传输操作中重点要考虑的问题。TCP/IP 协议是目前使用最为广泛的网络互联协议,但 TCP/IP 协议本身存在很多安全性问题,如何利用不安全的 TCP/IP 协议实现对数据的安全传输呢?最有效的方法就是对要传输的数据加密后传输。因此,作为网络安全管理与维护人员,要掌握数据的加密技术与方法,并能运用主流的加密与防护技术为企业的商业机密数据提供保护。

10.2 预 备 知 识

加密是对数据进行编码,使其转变为一种按常规不可理解的形式,这种形式称为密文。解密是加密的逆过程,即将密文还原成原来可以理解的形式。数据加密技术的关键是加密算法和密钥。加密算法是一组指令或一个数学公式,密钥则是算法中的可变参数。同一明文使用不同的加密算法,或使用相同的加密算法,但用不同的密钥,会得出不同的密文。衡量一个加密算法的可靠性,主要取决于解密的难度,而这与密钥长度有关。目前广泛应用的加密技术有两种,即对称密钥加密算法和非对称密钥加密算法,也称为私钥加密算法和公钥加密算法。

10.2.1 对称加密算法及其应用

对称加密也称为私钥加密体制。对称密钥加密技术使用相同的密钥对数据进行加密和解密,发送者和接收者使用相同的密钥。现在,对称加密算法有很多,通过特殊的数学算法实现强度增加,包括 DES 算法、IDEA 算法、3DES 算法、AES 算法、AED 算法、RC2 算法、RC4 算法、RC5 算法、Skipjack 算法和 Blowfish 算法等。一般从古典对称加密算法开始了解对称加密算法。

1. 古典对称加密算法

古典对称加密算法又称为恺撒加密。历史上恺撒南征北战,几乎统一了欧洲,奠定了罗马帝国。恺撒较早将此加密算法用于战争通信,用来保护重要军情,因此这种加密方法称为恺撒密码。恺撒密码的思想是将字母按顺序推后 3 位,从而起到加密作用,产生的明、密文对照表如下所示。

明文：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

密文：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

例如，信息“START WAR”用恺撒密码加密后变成了“VWDUW ZDU”，加密后的信息即使被敌方截获，也不会泄密。对于这种按字母顺序后移的加密算法，3是加密的密钥。如果改变加密密钥，明、密文对照表也会改变，比如把加密密钥改成5，则明文“STOP”转换成密文就是“XYTU”。显然，这种密码的加密强度是很低的，只需要简单统计字母频率就可以破译。

2. 现代对称加密算法

(1) 对称密钥加密技术的典型算法 DES

DES(Data Encryption Standard，数据加密标准)是最早、最著名的对称密钥加密算法，它由IBM公司在20世纪70年代发展起来的，于1977年被美国国家技术标准局(NIST)批准作为非机要部分使用的数据加密标准。在国内，DES算法在POS、ATM、磁卡及智能卡(IC卡)、加油站、高速公路收费站等领域被广泛应用，实现关键数据的保密。

DES的加密算法是公开的，保密性取决于对密钥的保密。DES是一个分组加密算法，分组长度为64位，密钥长度为56位，密钥是任意的56位数。就目前计算机的计算能力而言，DES不能抵抗对密钥的穷举搜索攻击，56位的密钥穷举数量是72亿次。

(2) 对称密钥加密技术的典型算法 3DES

三重DES(3DES)是DES的增强型，能有效运行168位密码。

(3) 对称密钥加密技术的典型算法 IDEA

IDEA(International Data Encryption Algorithm，国际数据加密算法)是一个迭代分组密码，分组长度是64位，密钥长度为128位。

(4) 对称密钥加密技术的典型算法 AES

为了替换安全性逐渐减弱的DES算法，2001年11月NIST公布Rijndael数据加密算法作为高级加密标准AES。AES的密钥长度可变，可以为128位、192位或256位，数据分组长度也可以指定为这三种。AES的强度至少和三重DES一样，但比三重DES更快。

3. 对称加密算法特点分析

对称加密算法的优点是加密处理简单，加密、解密速度快；在硬件加密的实现上较容易，成本也较低。例如，思科VPN集中器高端产品采用的是基于硬件加密，低端产品采用的是软件加密。其缺点是密钥管理困难，无法实施身份源认证。比如，有n个用户想实现两两加密通信，每一方至少要保管$n-1$个密钥，当用户量增多时，需要保管的密钥数更多。

10.2.2 非对称加密算法及其应用

非对称密钥加密算法又称为公钥和私钥算法，其特点是加密和解密使用不同的密钥。发送端用接收端的公钥加密数据后发送给接收端，接收端用自己的私钥解密。也就是说，用公钥加密的信息只能用与该公钥配对的私钥才能解密，用私钥加密的信息只能用与给定私钥配对的公钥才能解密，实现了对源的身份认证。因此，非对称加密算法的用途有两个，一是发送保密信息，不知道接收者私钥则无法窃取信息；二是确认发送者的身份，别人不知道发送者的私钥，无法发出能用其公钥解密的信息，因此发送者无法抵赖。目前主要的非对称

密钥算法(公钥算法)包括 RSA 算法、DSA 算法、PKCS 算法和 PGP 算法等。

1. 常见的非对称密钥加密技术的典型算法

(1) 非对称密钥加密技术的典型算法 RSA

RSA(算法以发明者 Ron Rivest、Adi Shamir 和 Leonard Adleman 的名字命名)公钥算法基于欧拉定理,经常应用于数字签名、密钥管理和身份认证等方面,适用于数字签名和密钥交换。该算法的安全性建立在大素数分解的基础上。素数分解是一个极其困难的问题。

(2) 非对称密钥加密技术的典型算法 DSA

DSA 算法仅适用于数字签名。路由器配置 VPN 中常用的非对称加密算法主要是 RSA 和 DEA。这两种算法主要用于数字签名,即进行源认证,根本原理是私钥加密签名,对应的公钥进行验证。

2. 非对称密钥加密算法的特点

非对称密钥加密算法解决了密钥管理问题,通过特有的密钥分发算法,使得当前用户数大幅度增加时,密钥数增加也不会很离谱。由于密钥事先已经分配,不需要在通信过程中传输,安全性大大提高,并且它具有高加密强度。其缺点是加密算法复杂,加密、解密的速度很慢。

3. 非对称加密算法工具软件 PGP

PGP(Pretty Good Privacy)是信息安全传输领域的加密软件,技术上采用了非对称的公钥和私钥加密算法。软件的主要对象为具有一定商业机密的企业、政府机构、信息安全工作室。PGP 最初的设计主要是用于邮件加密,如今发展到可以加密文件、文件夹、分区、硬盘,甚至对聊天信息进行实时加密,只要双方都安装了 PGP,就可以在聊天的同时进行加密或解密,保证聊天信息不被窃取或监视。

10.2.3　分析对比对称加密和非对称加密算法

对称加密算法具有加密速度快、运行时占用资源少等特点;非对称加密算法可以用于密钥交换,密钥管理安全。通常并不直接使用非对称加密技术,因为非对称加密算法的处理速度慢很多,当有大量数据要进行加密处理时会降低数据的传输速率,但用非对称加密算法加密一个对称密钥还是很快的。

常见的密钥分发技术有 CA 技术和 KDC 技术。CA 技术能够完成公钥和对称密钥的分发,KDC 技术用于对称密钥分发。

EFS(Encrypting File System)加密文件系统是 Windows XP/2003 等系统特有的实用功能,对于 NTFS 卷上的文件和数据,都可以直接加密保存。EFS 采用扩展的数据加密标准(DESX)56 位加密算法。加密的方法是选中 NTFS 分区中的一个文件,然后右击;选择"属性"命令,在出现的对话框中单击"常规"选项卡,然后单击"高级"按钮;在出现的对话框中选中"加密内存以便保护数据"选项,然后单击"确定"按钮。

也可使用 cipher 命令,显示或更改 NTFS 分区上的文件的加密。例如,如果想加密 C 盘下的 GL 文件夹,输入"cipher /e C:\GL";解密时输入"cipher /d C:\GL"。

EFS 保护文件的工作原理是基于非对称公钥算法和对称公钥算法的混合算法。文件使用对称算法加密;文件的加密密钥使用用户证书的公钥加密,并与加密的文件一起存储。用户的私钥可解密出文件的加密密钥,然后解密文件。

为了保证数据的安全，最好能在加密文件之后立即将自己的密钥备份出来，特别是在系统重装之前，一定要进行如下操作：单击“开始”→“运行”菜单项，在出现的对话框中输入“certmgr.msc”，按“Enter”键后，在出现的“证书”对话框中依次双击展开“证书”→“当前用户”→“个人”→“证书”选项，可以看到一个以当前的用户名为名称的证书。右击该证书，在“所有任务”中单击“导出”并选择“导出私钥”，导出的证书将是一个以 pfx 为后缀的文件。当用户的密钥丢失后，如重装了操作系统，或者无意中删除了某个账号，只要找到之前导出的 pfx 文件，右击并选择“安装 Pfx”，将弹出导入向导，按照导入向导的指示完成操作，之前加密的数据可以全部正确打开。

注意：如果之前在导出证书时选择了用密码保护证书，在导入证书时就需要提供正确的密码，否则将不能继续。

目前出现了 EFS 加密的破解软件 Advanced EFS Data Recovery(AEDR)，破解率很高。但这对于重装 C 盘系统后的情况不适用，因为它破解的前提是私钥在当前主机系统的硬盘中存在，或者有备份。需要注意的是，因为 EFS 的高安全性，如果用户操作不当，很可能导致数据丢失。

10.2.4 认证技术

认证是为了防止恶意者的主动攻击，其包括检验信息的真伪及防止信息在通信过程中被篡改、删除、插入、伪装、延迟和重放等。认证主要包括三个方面：消息认证、数字签名和身份认证。消息认证是指验证所收到的消息确实是来自真正的发送方，并且是未被修改过的，也可以验证消息的顺序和及时性。消息认证不一定是实时的，如存储系统和电子邮件系统。身份认证用于鉴别用户的身份是否是合法用户，常用的方法包括口令认证、持证认证和生物识别。国际电信联盟(ITU)和 IETF 制定了认证中心的标准 ITU X.509。

账户名/口令认证方式是被广泛研究和使用的一种身份验证方法，也是认证系统所依赖的一种最实用的机制，常用于操作系统登录、Telnet 等。常用的身份认证协议主要有一次一密机制、X.509 认证协议、Kerberos 认证协议等。Kerberos 是为 TCP/IP 网络设计的可信第三方鉴别协议。Kerberos 基于对称密钥机制，一般采用 DES 算法，也可以采用其他算法。在 Kerberos 模型中，实体是位于网络上的客户机和服务器。客户机可以是用户，也可以是处理事务所需要的独立的软件程序。Kerberos 有一个存有所有用户秘密密钥的数据库。对于每个用户而言，秘密密钥是一个加密口令(即加密以后的用户密码)。Kerberos 能提供会话密钥，只供一台客户机和一台服务器(或两台客户机之间)使用。会话密钥用来加密双方间的通信信息，通信完毕应立即销毁。常见的散列函数有 MD5 和 SHA-1。MD5 算法通过填充、附加、初始化累加器、进行主循环 4 步处理得到 128 位消息摘要。安全哈希算法(SHA-1)用于产生一个 160 位的消息摘要。

10.2.5 数字证书技术

数字证书封装了用户自身的公钥等信息，例如 X.509 数字证书包含了证书版本、证书序列号、签名算法标识、证书有效期、证书发行商名字、证书主体名、证书公钥信息和数字签名等元素。使用某个数字证书对数据进行加密，就是使用该数字证书中的公钥对数据进行加密。

数字签名是笔迹签名的模拟，包括了消息认证函数，具有的性质包括：必须能证实作者

签名和签名的日期及事件,在签名时必须能对内容进行鉴别,签名必须能被第三方证实以解决争端。基于公钥密码体制和基于私钥密码体制都可以获得数字签名,目前主要是基于公钥密码体制的数字签名。利用公钥密码体制,数字签名是一个加密的消息摘要,附加在消息的后面。基于公钥密码体制的数字签名是指以用户的私钥作为加密密钥,以公钥作为解密密钥,从而实现由一个用户加密的消息能够被多个用户解读,且发送方无法否认自己所发送的信息。

广泛使用的安全电子邮件技术包括 PGP 和 S/MIME(安全/通用 Internet 邮件扩充)。摘要函数是安全电子邮件实现技术之一。一个好的摘要函数具有如下特点:根据输入报文获取其输出摘要的时间非常短,根据输入数据无法还原出输入数据,不同长度的输入报文计算出的摘要长度相同。

10.3　方案设计

方案设计如表 10-1 所示。

表 10-1　方案设计

任务名称	数据加密技术的使用
任务分解	1. PGP 系统安装 (1) 软件安装 (2) 密钥对的生成和查看 (3) 重新创建密钥对 (4) 导出并发布自己的公钥 (5) 导入并设置其他人的公钥 2. 使用 PGP 系统加密数据文件 (1) 加密和解密 (2) 签名和验证 (3) 加密和签名 3. 使用 PGP 系统加密邮件 (1) 加密和签名 (2) 解密和验证签名 4. 使用 PGP 系统加密本地硬盘 (1) 创建加密磁盘 (2) 加载加密磁盘 (3) 卸载加密磁盘
能力目标	1. 能安装 PGP 系统 2. 能生成和查看公钥和私钥 3. 能重新创建密钥对 4. 能导出并发布自己的公钥 5. 能导入其他人的公钥,并设置公钥属性来获得信任关系 6. 能使用 PGP 系统加密和解密文件 7. 能对文件进行签名和签名验证 8. 能使用 PGP 系统加密和签名邮件 9. 能使用 PGP 系统解密和验证签名邮件 10. 能使用 PGP 系统创建加密磁盘、加载加密磁盘和卸载加密磁盘

续表

知识目标	1. 掌握密码学的有关概念 2. 了解常见的古典密码加密技术 3. 理解对称加密算法和非对称加密算法的基本思想以及两者的区别 4. 了解对称密钥加密技术的典型算法 DES、3DES、IDEA 和 AES 5. 熟悉对称加密算法的特点和优、缺点 6. 了解非对称加密技术的典型算法 RSA 7. 熟悉非对称加密算法的特点和优、缺点 8. 了解非对称加密算法攻击软件 PGP 加密系统的工作原理、密钥的生产和管理方法以及各种典型的应用 9. 理解 PGP 加密系统中密钥信任关系的传递特性 10. 了解非对称密钥算法和对称密钥算法的混合算法 EFS 的工作原理 11. 熟悉 EFS 加密文件系统的使用方法
素质目标	1. 树立较强的安全意识 2. 掌握网络安全行业的基本情况 3. 培养良好的职业道德 4. 培养职业兴趣，以及爱岗敬业、热情主动的工作态度 5. 具有可持续发展能力

10.4 任务实施

10.4.1 任务1：PGP系统安装

1. 任务目标

安装 PGP 系统。

2. 工作任务

（1）软件安装；

（2）密钥对的生成和查看；

（3）重新创建密钥对；

（4）导出并发布自己的公钥；

（5）导入并设置其他人的公钥。

3. 工作环境

（1）两台预装 Windows Server 2003/XP 的主机，通过网络相连。

（2）软件工具：PGP 加密软件。

4. 实施过程

（1）软件安装

软件的安装很简单，具体步骤如下：

① 双击或运行安装程序，进入安装界面，将显示欢迎信息，然后单击“Next”按钮。

② 在弹出的许可协议窗口，阅读后选择接受，单击“Yes”按钮。继续单击“Next”按钮，

出现创建用户类型的界面，再单击“Next”按钮。

③ 安装程序提示用户是否已经有密钥。如果安装过 PGP，可能在计算机中存在密钥；如果没有安装过，选择“No，I’m a New User”，如图 10-1 所示。

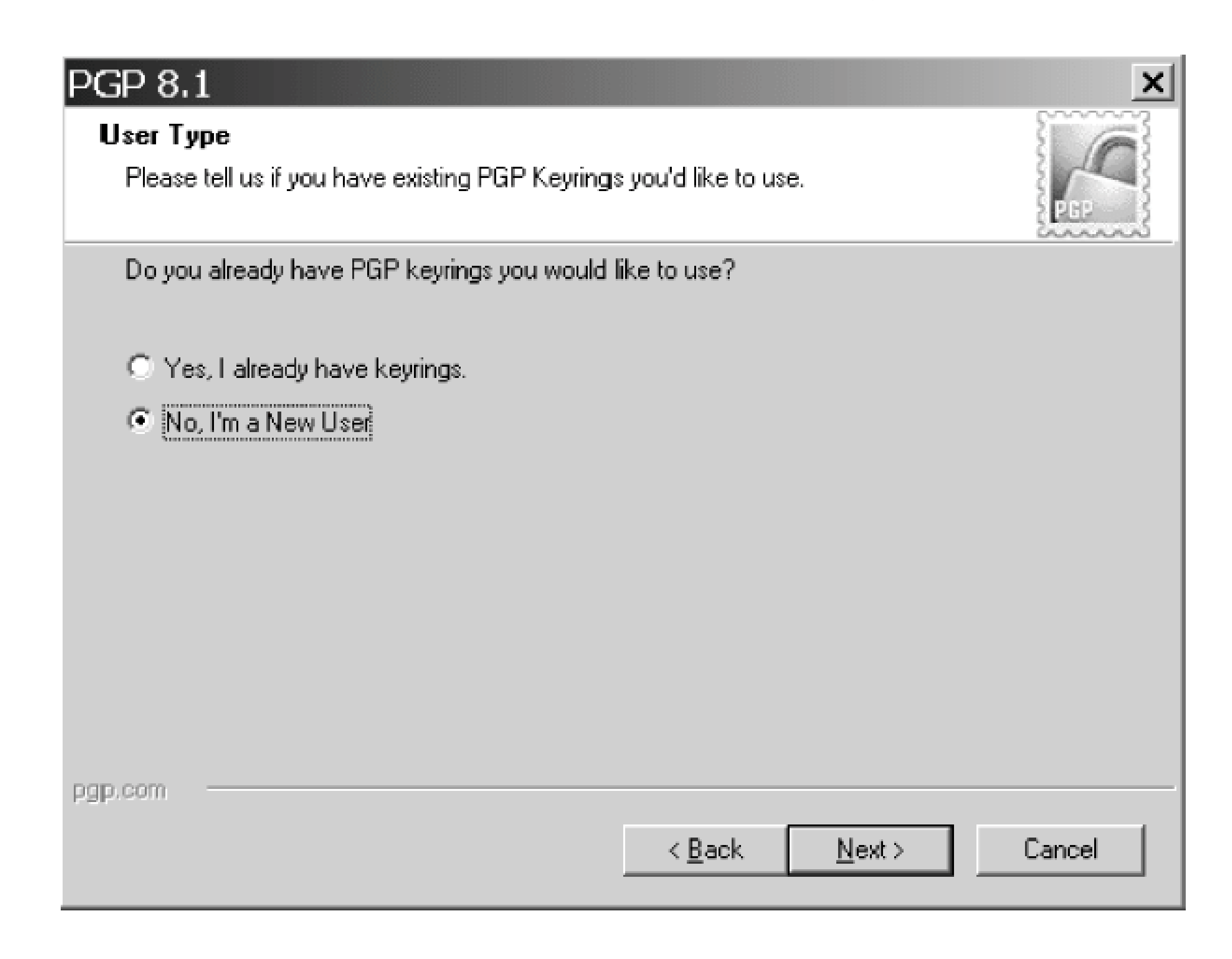


图 10-1　用户类型的选择

④ 单击“Next”按钮，出现程序的安装目录。建议将 PGP 安装在安装程序默认的目录，即系统盘中。

⑤ 继续单击“Next”按钮，出现选择 PGP 组件的窗口，安装程序会支持系统内所安装的程序。如果存在 PGP 可以支持的程序，它将自动选中该支持组件，如图 10-2 所示。

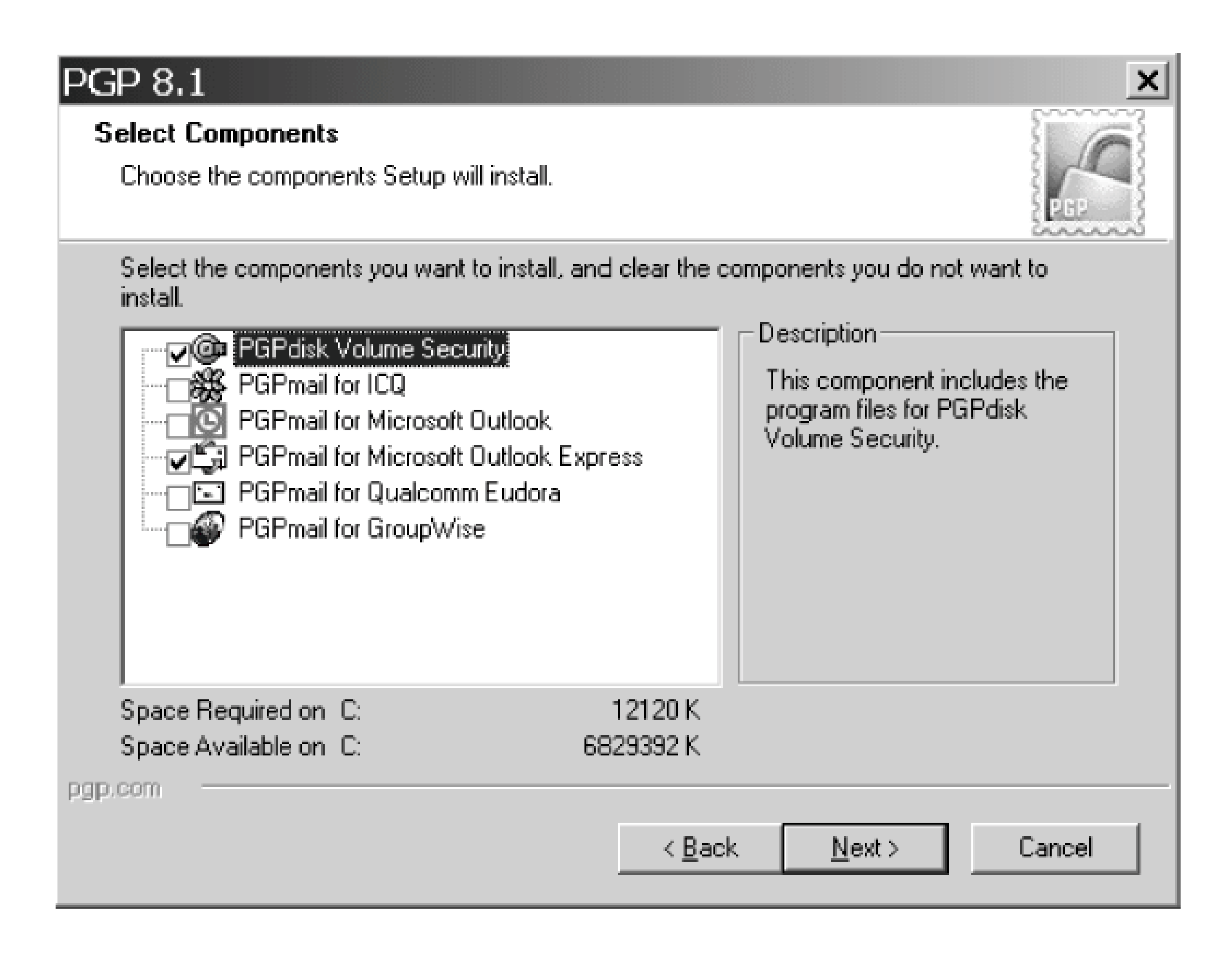


图 10-2　“Select Components”对话框

⑥ 按提示单击“Next”按钮，重启系统即完成安装。

⑦ 重启后，系统会启动 PGP 许可验证，PGP 已经在“开始”→“程序”→“启动”中加入了启动项。在“PGP License Authorization”认证对话框中输入“Name”、“Organization”、“License Number”等信息，然后单击“Manual”按钮。在文本框内输入“License Authorization”信息，单击“Authorize”按钮完成注册；也可以选择试用，即什么信息都不填，直接单击“Later”

按钮。

⑧ 弹出“PGP License”窗口,单击“OK”按钮。至此,PGP系统安装完毕。

(2) 密钥对的生成和查看

① 安装完成并重新启动系统后,会出现“PGP Key Generation Wizard”即“密钥生成向导”对话框,要求输入用户全名和邮箱地址,如图10-3所示。这里不需要输入真实的名称,但是输入一个其他人看得懂的名字,能使他们在加密时很快找到想要的密钥。

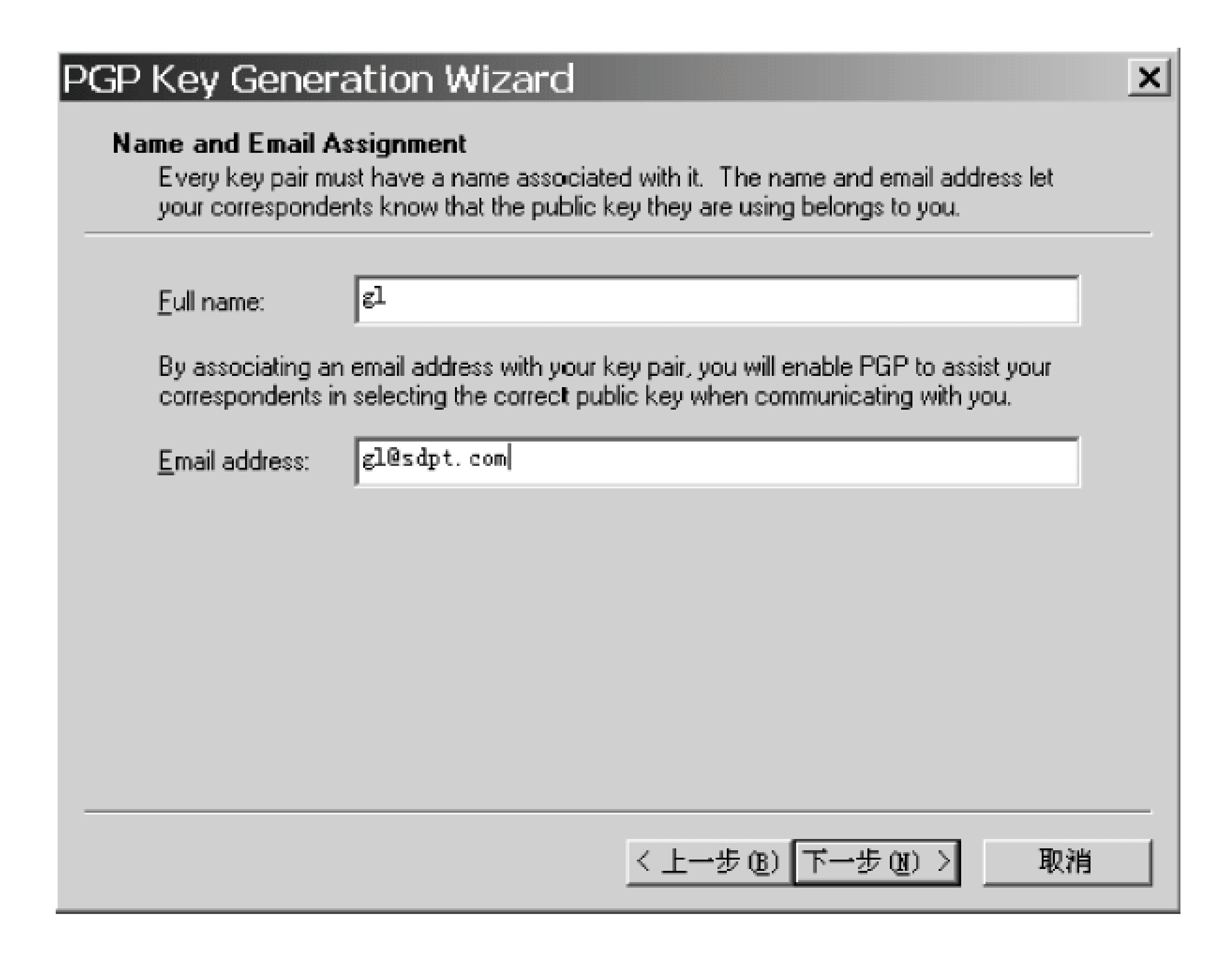


图10-3 个人信息填写

② 单击“下一步”按钮,弹出的对话框要求输入用于保护私钥的密码。此密码长度建议在8位以上,并要求确认,即重复一遍,即在“Passphrase”处输入密码,“Confirmation”处重复一遍输入的密码。右上角的“Hide Typing”被选中,则输入的密码不会显示出来,如图10-4所示。为了方便记忆,可以用一句话作为密码。

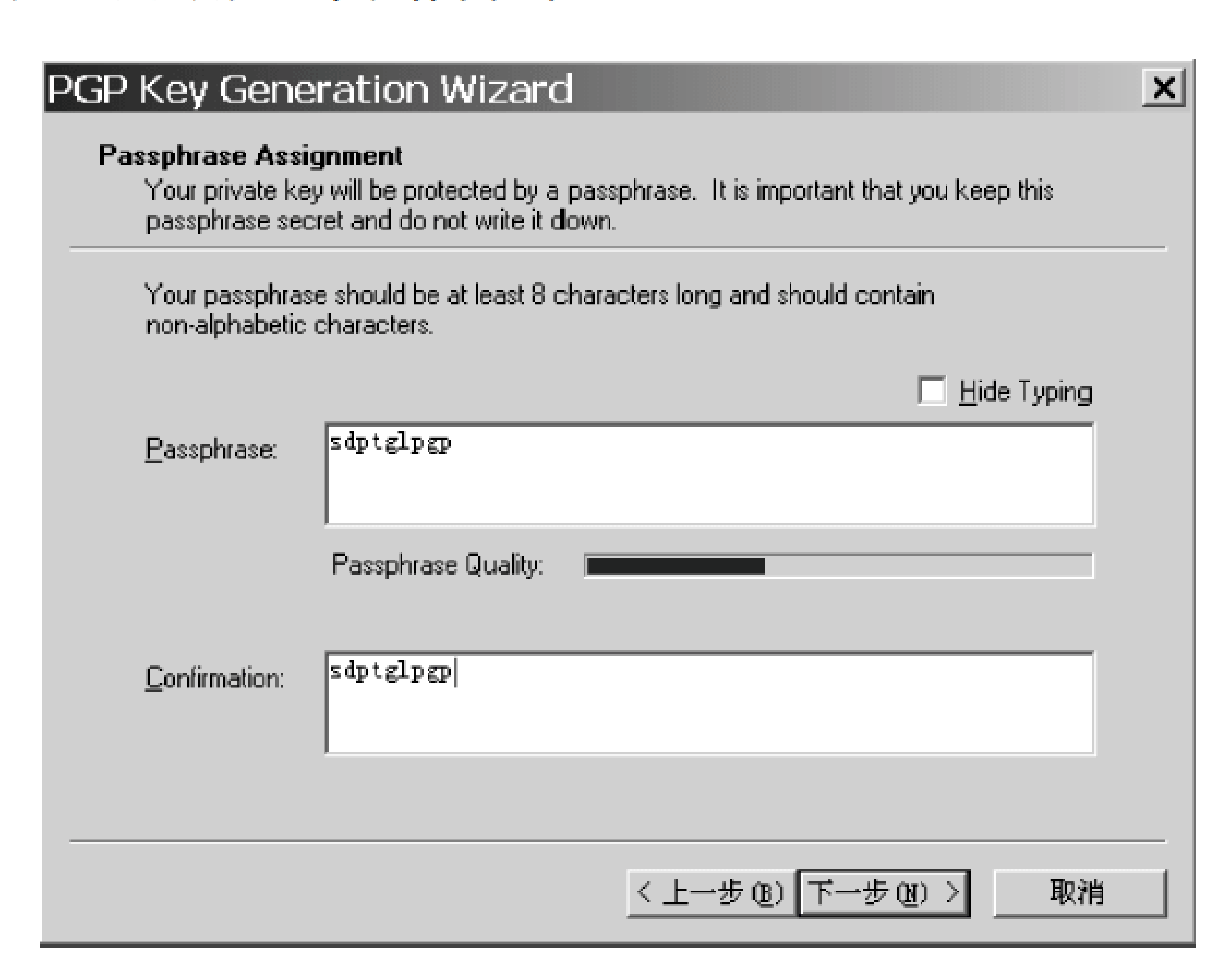


图10-4 保护私钥的密码设置

③ 进入“Key Generation Progress”即密钥生成阶段,等待主密钥(Key)和次密钥(Subkey)生成完毕(Done),然后单击“下一步”按钮。

④ 继续单击“下一步”按钮，进入“Completing the PGP Key Generation Wizard”，即完成该 PGP 密钥生成向导。再次单击“完成”按钮，密钥被创建并设置好。

⑤ 通过“开始”程序中的 PGP 启动“PGPKeys”，可以看到已经创建好的密钥及其基本信息，例如 Validity(有效性，PGP 系统检查是否符合要求，符合就显示为绿色，否则为灰色)、Trust(信任度)、Size(大小)、Description(描述)、Key ID(密钥 ID)、Creation(创建时间)、Expiration(到期时间)等，如图 10-5 所示。

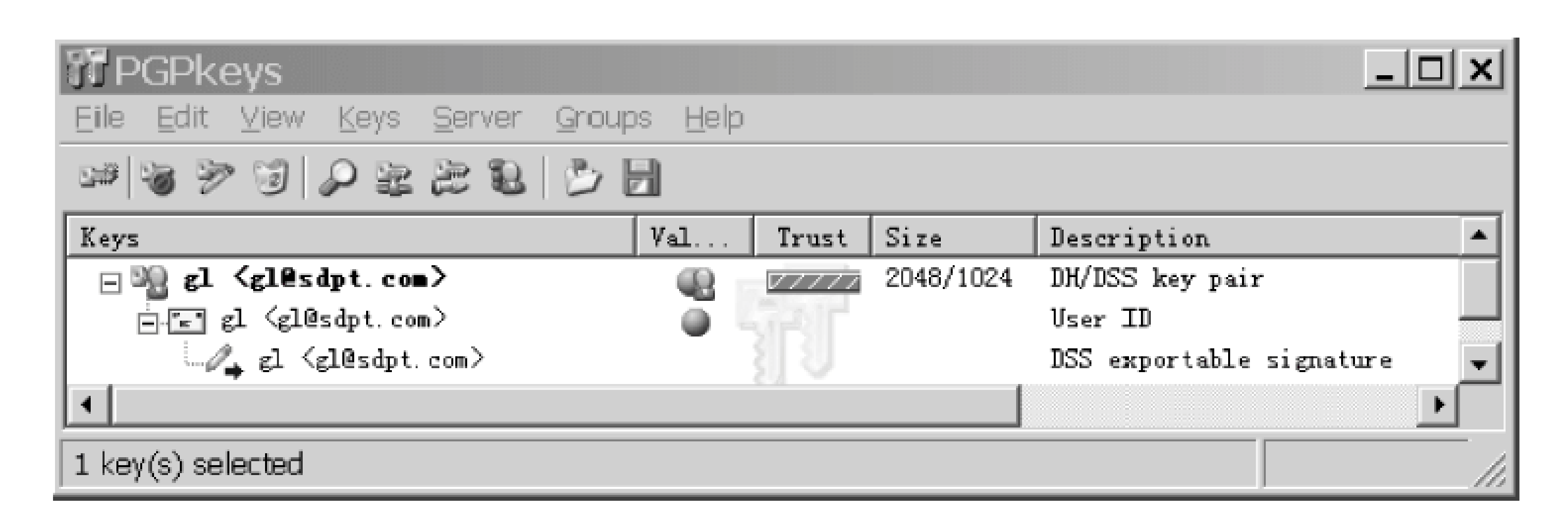


图 10-5　“PGPkeys”窗口

⑥ 右击密钥 gl 的“Key properties”菜单项，可以在一个窗口中看到所有属性，如图 10-6 所示。

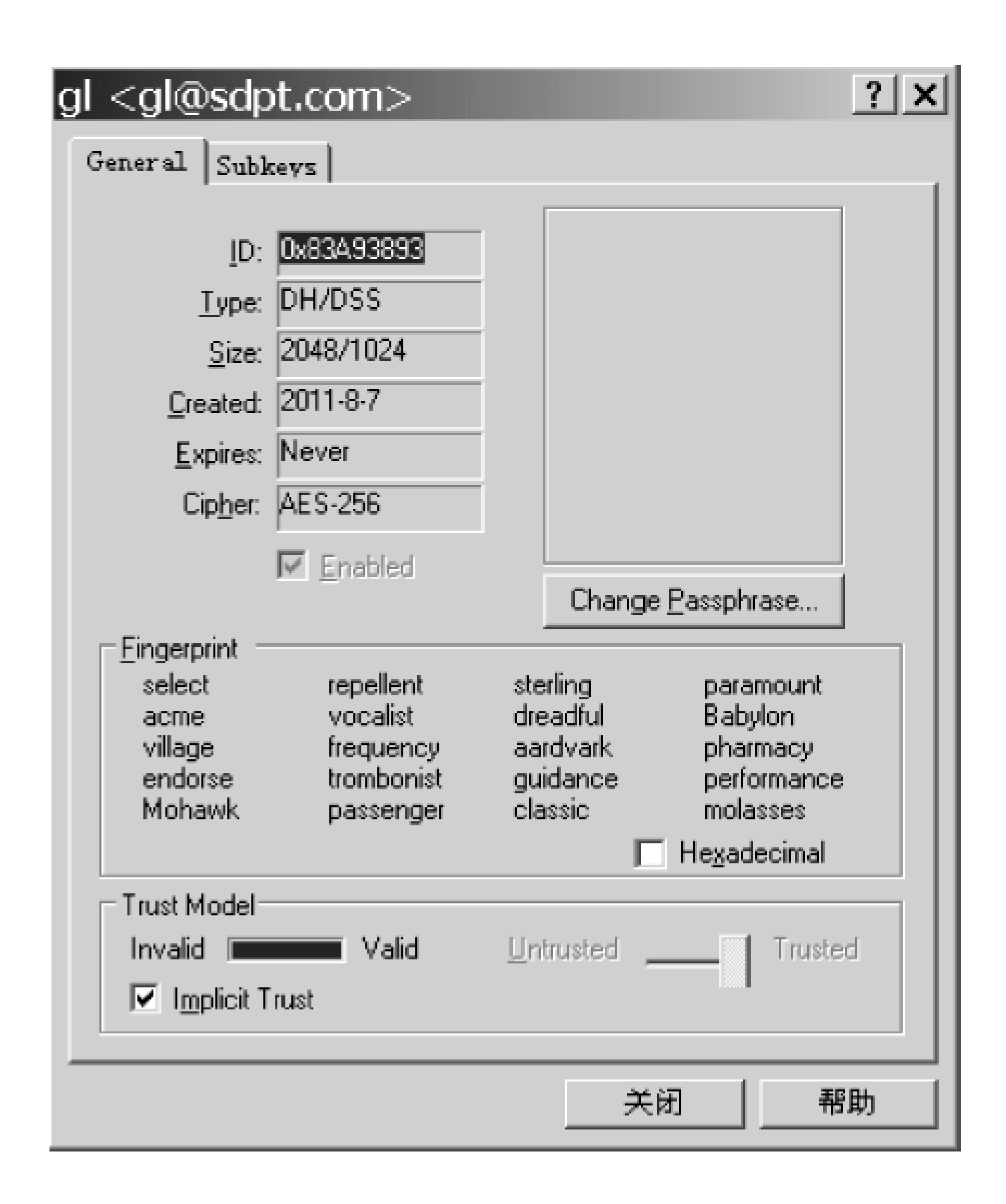


图 10-6　密钥属性查看

(3) 重新创建密钥对

单击 PGP 程序窗口中“Keys”菜单中的“New Key”菜单项，可以重新生成一对密钥，即公钥和私钥对(Key pair)，如图 10-7 所示。

(4) 导出并发布自己的公钥

通过 PGP 程序窗口中的“Keys”菜单，选择“Export”选项，可以导出当前选中的密钥对中的公钥。需要注意的是，一个用户对应的密钥以“密钥对”的形式存在，其中包含了一个公钥和一个私钥。公钥可以分发给任何人，其他人可以用此密钥对要发给此密钥拥有者的文

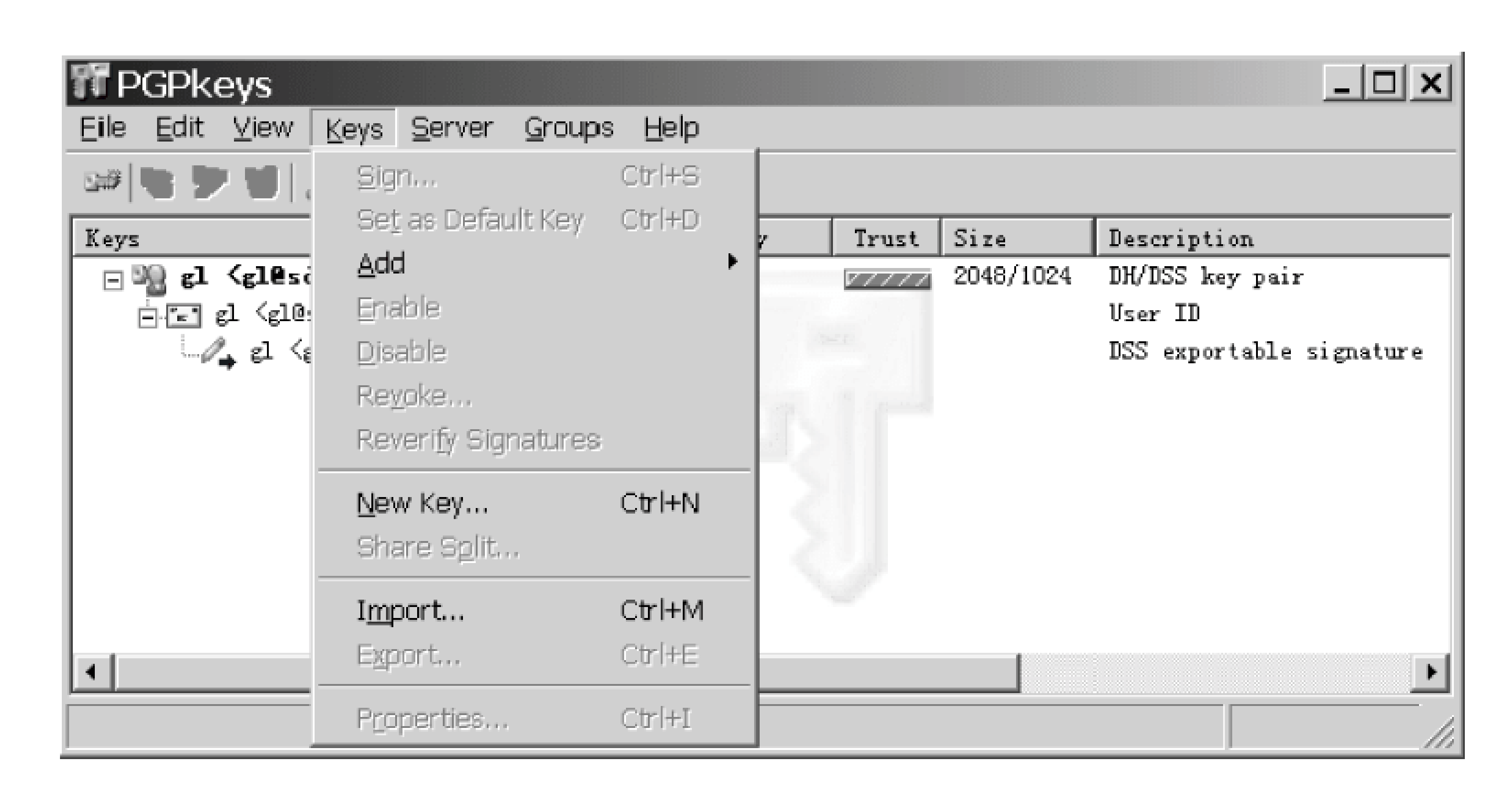


图 10-7 重新创建密钥对

件或邮件进行加密。私钥只有此密钥的拥有者一人所有，不可公开分发，此密钥用来解密所有用此密钥拥有者的公钥加密的文件或邮件。如果在导出到文件的窗口下面选中“Include Private Key”，则导出了公钥和私钥。一般情况下，不需要导出私钥。

导出公钥的具体操作步骤如下：

① 右击窗口中的密钥对，在弹出的快捷菜单中选择“Export...（导出）”。

② 在弹出的保存对话框中，确认只选中了“Include 6.0 Extensions（包含 6.0 公钥）”，然后选择一个目录作为导出公钥存放的目录，最后单击“保存”按钮，如图 10-8 所示。

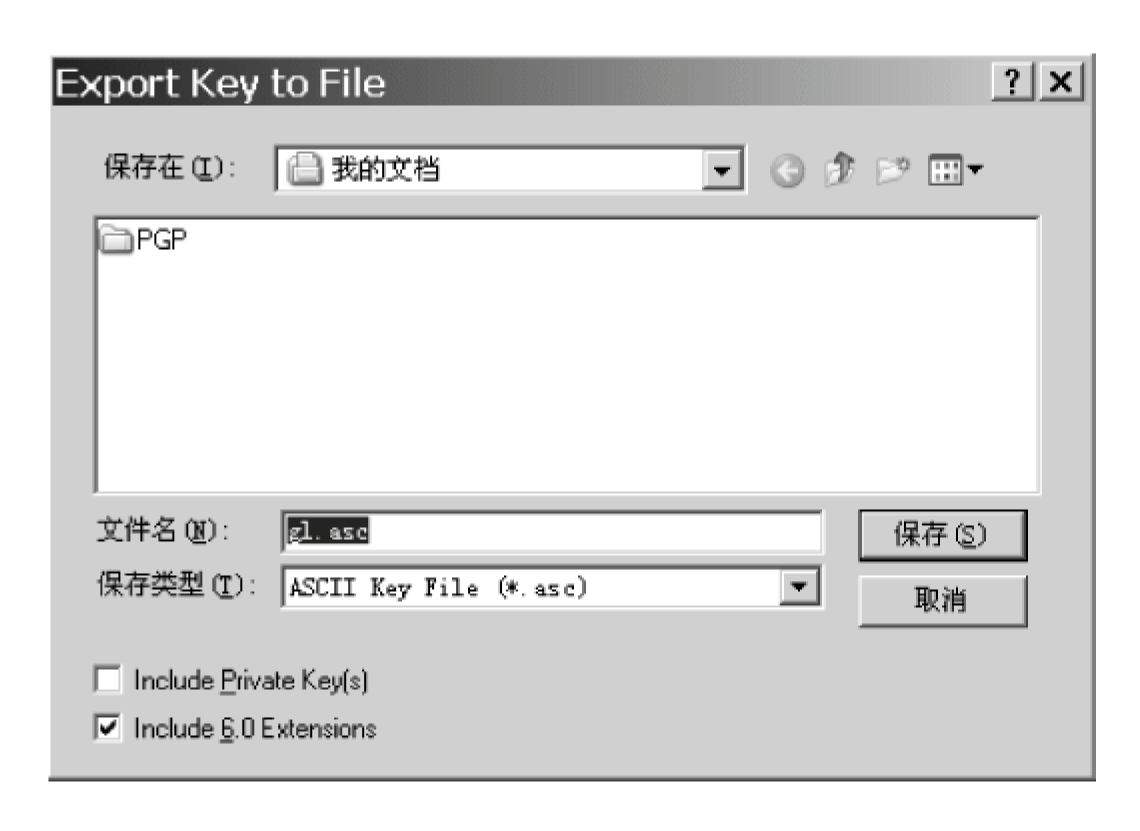


图 10-8 导出密钥

③ 导出公钥，扩展名是.asc。

导出后，可以将此公钥发布出去，发给通信的对方。当有重要的文件或邮件时，对方通过 PGP 使用此公钥加密后发回来，这样能防止隐私或商业机密被窃取，即便被截获也很难解密。

(5) 导入并设置其他人的公钥

导入公钥的方法如下：

① 直接双击对方发来的扩展名为.asc 的公钥，将会出现选择公钥的窗口，在此能看到该公钥的基本信息，包括有效性、创建时间、信任度等，便于了解是否应该导入此公钥。

② 选好后，单击“Import”（导入）按钮，即可把公钥导入到 PGP 中。

导入其他人的公钥后，显示“无效的”并且是“不可信任的”，表示新导入的公钥还没有得到用户的认可。如果确信这个公钥是正确的，即没有被第三方伪装或篡改，可以通过设置公钥属性来使之获得信任关系。

设置公钥属性的方法如下：

① 打开“PGPkeys”对话框，在密钥列表中看到刚刚导入的密钥。选中后右击，然后选择“Key Properties”（密钥属性），在这里能看到该密钥的全部信息。

② 直接拉动“Untrusted（不信任的）”的滑块到“Trusted（信任的）”，将出现错误信息，如图 10-9 所示。



图 10-9　错误提示

③ 正确的做法是关闭此对话框，然后在该密钥上右击，再选择“Sign（签名）”，打开“PGP Sign Key”对话框，如图 10-10 所示。

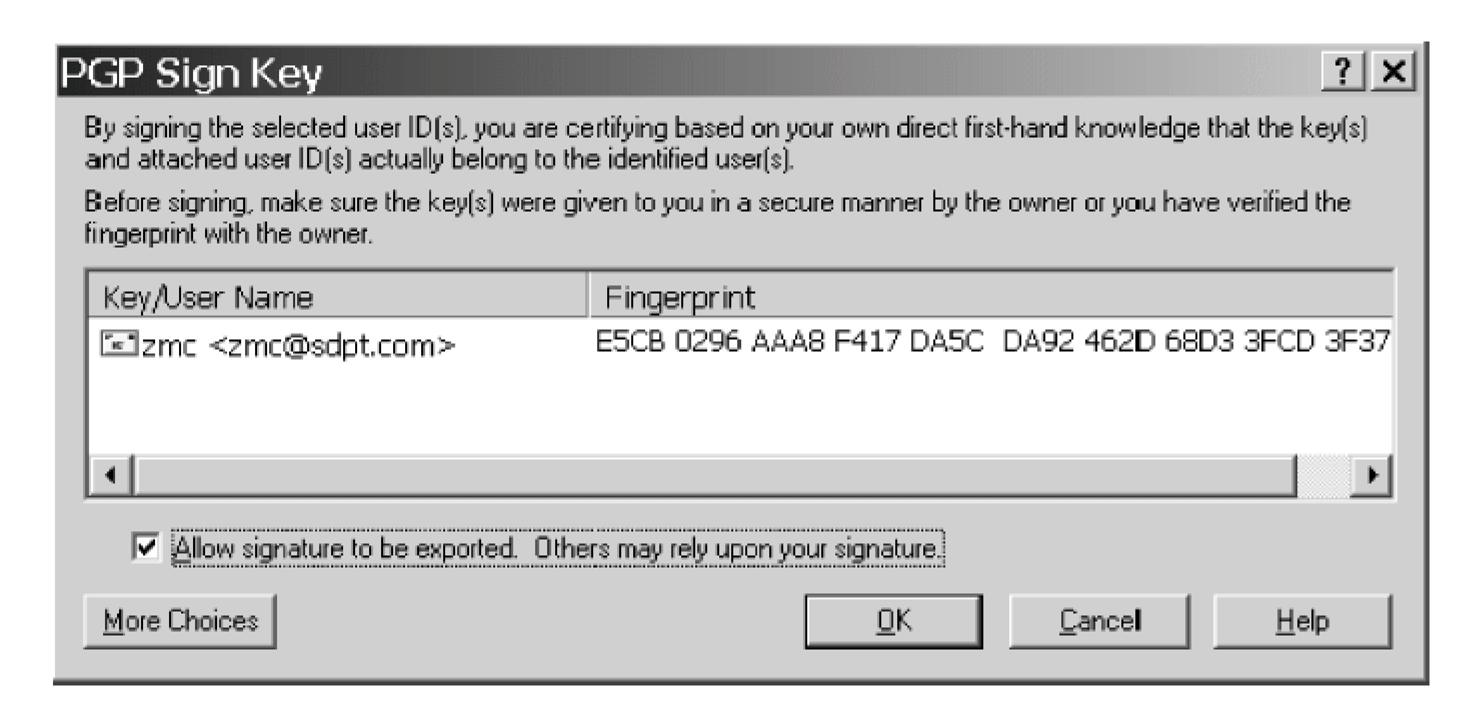


图 10-10　对新导入的公钥进行签名

④ 在出现的“PGP Sign Key”（PGP 密钥签名）对话框中选中要签名的公钥，并选中“Allow signature to be exported. Others may rely upon your signature”，然后单击“OK”按钮。

⑤ 弹出要求为该公钥输入 Passphrase 的对话框，这时要输入设置用户时的那个密码，然后单击“OK”按钮，完成签名操作，如图 10-11 所示。

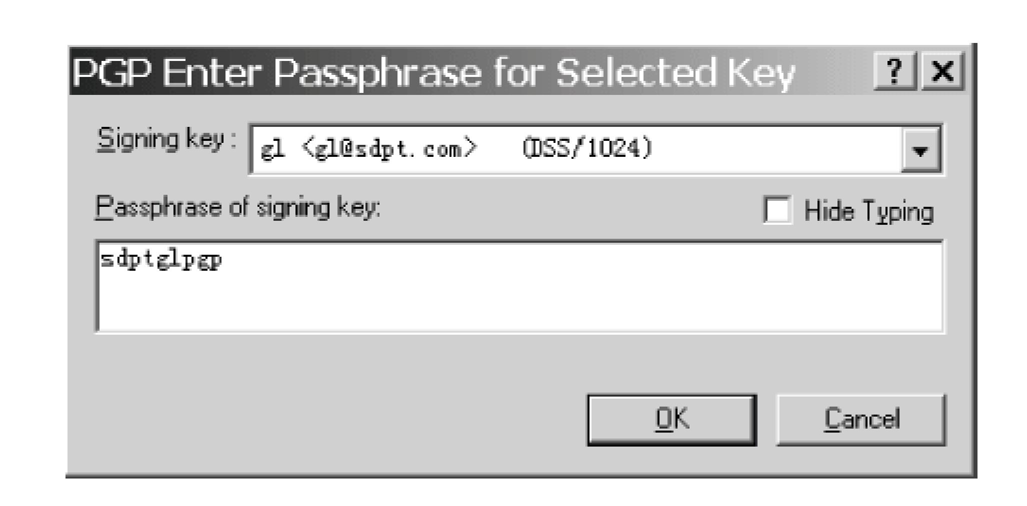


图 10-11　输入密码

⑥ 此时，在“PGPkeys”对话框中，该公钥变成“有效的”，即在“Validity”栏出现绿色圆球标志，如图 10-12 所示。此时该公钥是“不可信任的”，需要对其赋予完全信任关系。

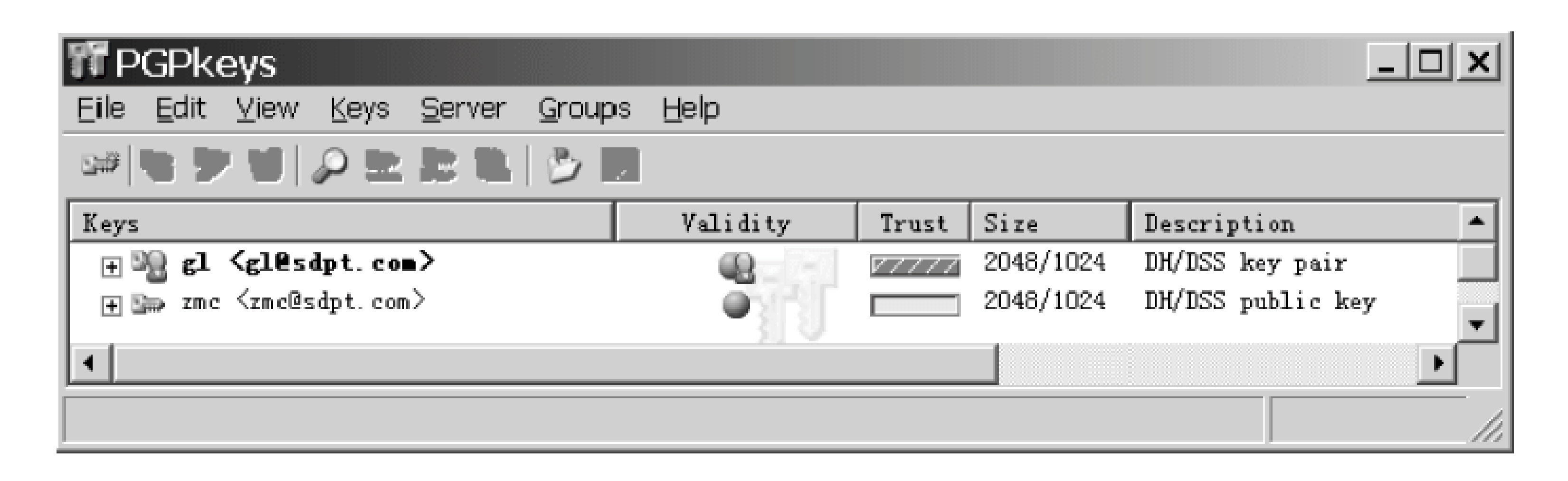


图 10-12 签名后的公钥状态

⑦ 右击该公钥，然后选择“Key Properties”（密钥属性），将“Untrusted”（不信任的）处的滑块拉到“Trusted”（信任的）处，再单击“关闭”按钮，如图 10-13 所示。这时，密钥列表里的公钥“Trust”（信任度）处变成一个实心栏，说明该公钥被 PGP 加密系统正式接受，可以投入使用了，如图 10-14 所示。

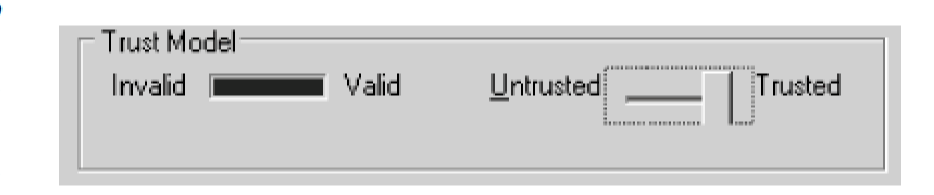


图 10-13 对密钥赋予信任关系

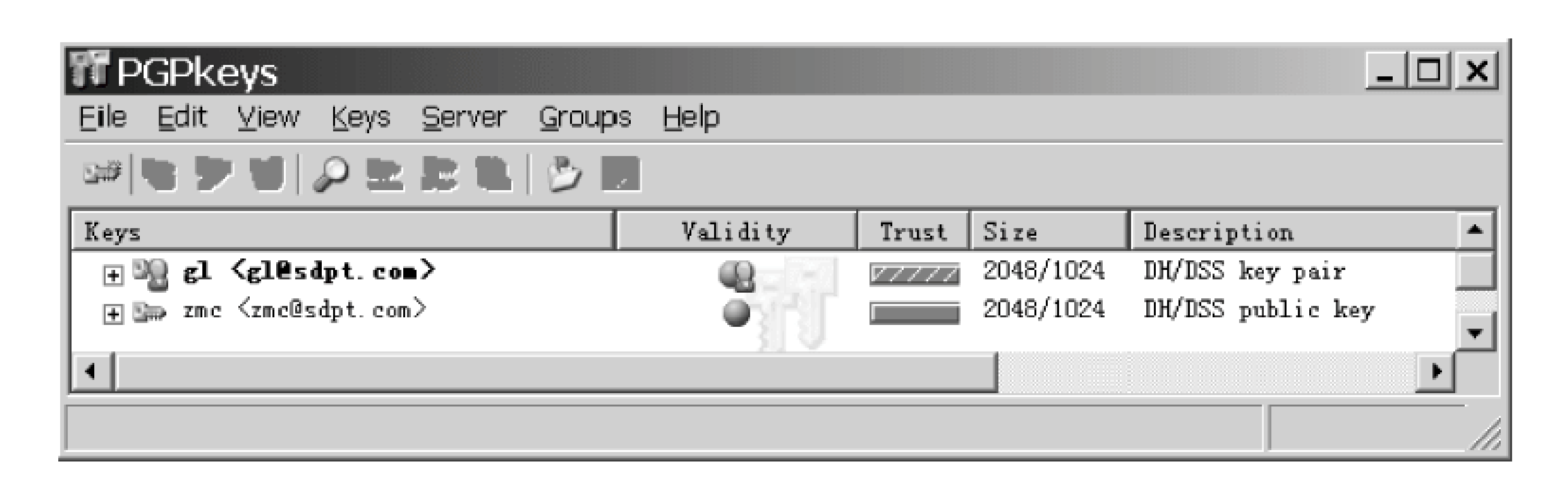


图 10-14 签名并赋予完全信任关系后的公钥

10.4.2 任务 2：使用 PGP 系统加密数据文件

1. 任务目标

使用 PGP 对数据文件进行加密、签名的操作原理是选择对方的公钥进行加密，而使用自己的私钥进行签名；对方收到后，使用自己的私钥进行解密，使用对方的公钥进行签名验证。

2. 工作任务

(1) 加密和解密；

(2) 签名和验证；

(3) 加密和签名。

3. 工作环境

(1) 两台预装 Windows Server 2003/XP 的主机。

(2) 软件工具：PGP 加密软件。

4. 实施过程

(1) 加密和解密

使用 PGP 对文件加密非常简单,具体操作如下:

① 右击需要加密的数据文件,然后选择快捷菜单中 PGP 的 Encrypt 命令,弹出如图 10-15 所示对话框。

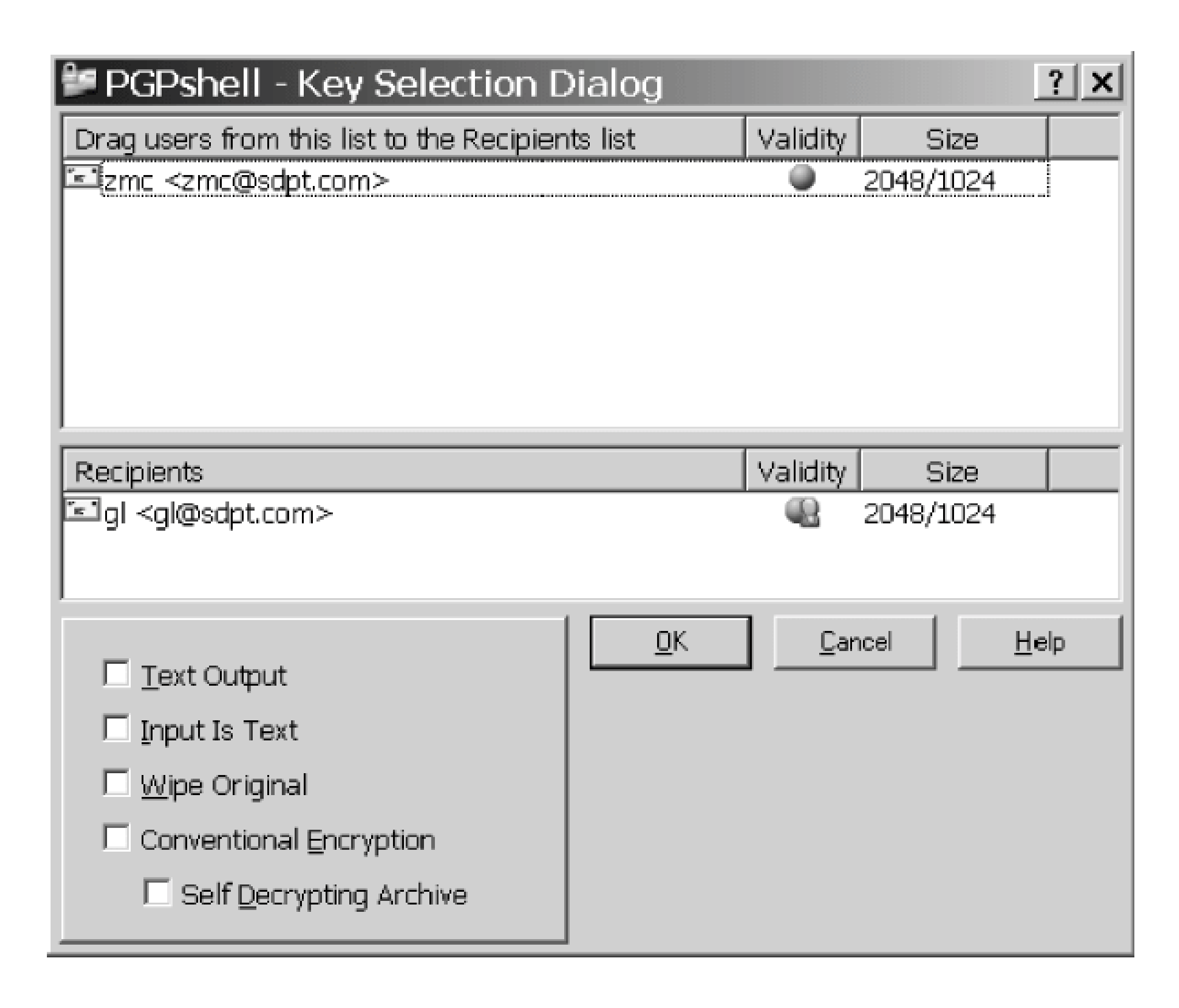


图 10-15　“选择密钥”对话框

② 在弹出的“Key Selection Dialog”对话框中,选择对方的密钥,双击使其加到下面的“Recipients”框中,即使用公钥加密,然后单击“OK”按钮,如图 10-16 所示。

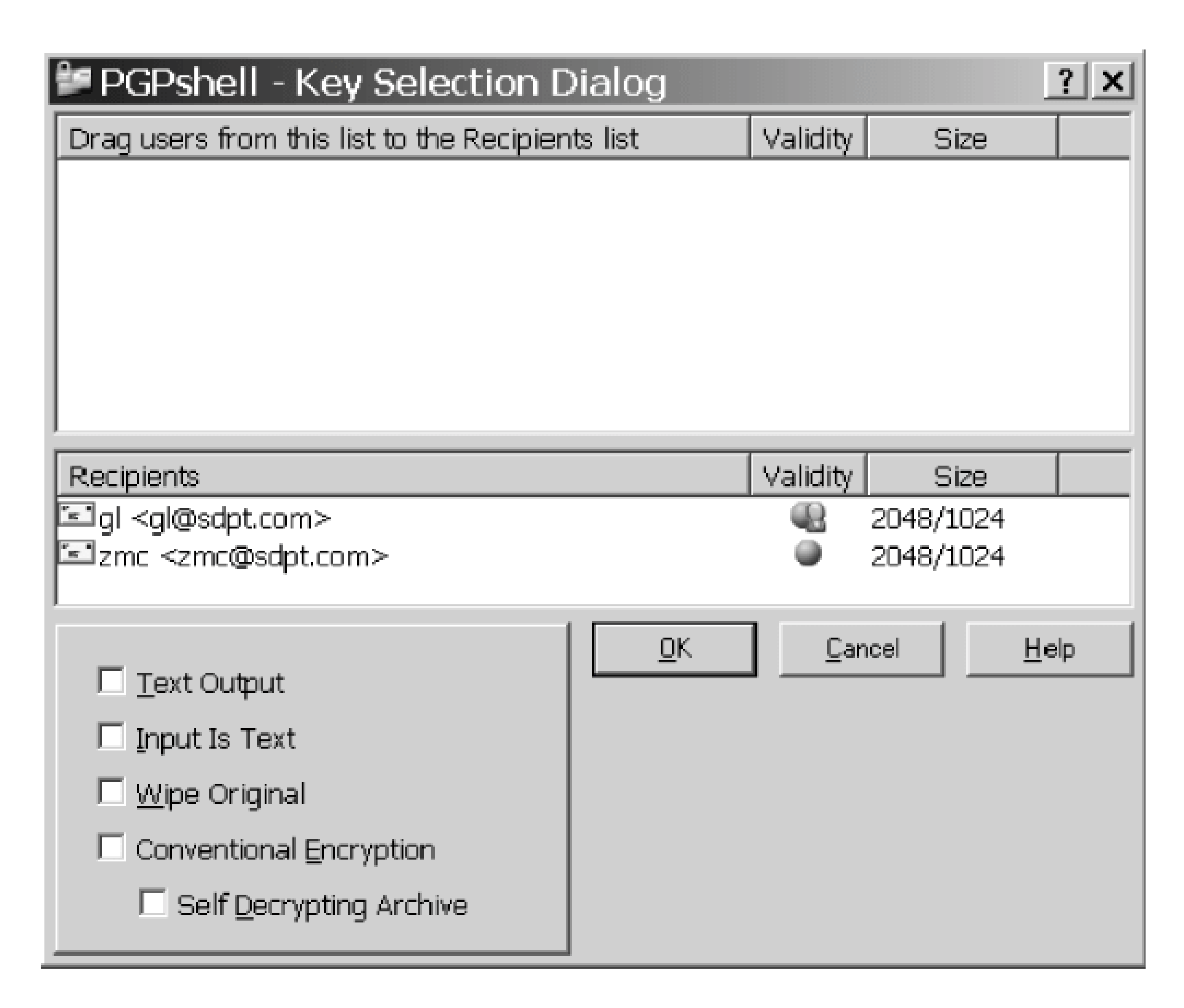


图 10-16　选择加密的公钥

③ 加密后产生一个扩展名为.pgp 的文件。

④ 对方收到加密的扩展名为.pgp 的文件后,双击该文件,或右击该文件,并选择快捷菜单中 PGP 的 Decrypt 命令,然后在对话框中输入密码,即使用私钥解密。

(2) 签名和验证

① 如果要对文件进行签名,右击需要签名的文件,然后选择快捷菜单中 PGP 的 Sign 命令,弹出如图 10-17 所示对话框。

② 输入自己私钥的密码,签名后产生扩展名为.sig 的文件。

③ 对方把公钥导入,并把公钥的属性设置成“有效的”、“可信任的”,详见 10.4.1 小节“导入并设置其他人的公钥”任务说明。

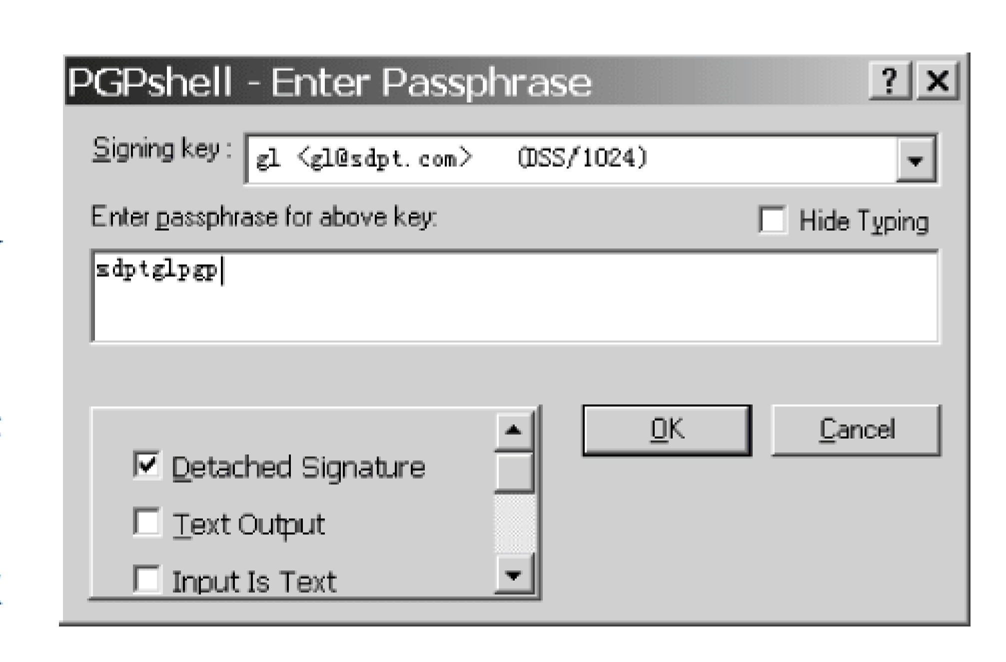


图 10-17 使用 PGP 对文件进行签名

④ 对方导入并设置完公钥后进行签名验证。签名验证成功,显示如图 10-18 所示对话框,从中可以看到签名状态是否完好。



图 10-18 使用 PGP 成功对文件进行签名验证

⑤ 如果文件在传送过程中被第三方伪装或篡改,则签名验证不成功,显示为“Bad Signature”。

⑥ 如果对方没有对公钥进行签名并赋予完全信任关系,那么验证签名后会在“Validity”栏显示一个灰色的图标,如图 10-19 所示,表示该签名验证无效。



图 10-19 没有对公钥进行签名并赋予完全信任关系时验证文件签名情况

需要特别注意的是,将签名后的.sig 文件传送给对方的同时,必须将原始文件也传送给他,否则签名验证将无法完成。这是因为 PGP 签名时只对原始文件的摘要进行签名,对方打开.sig 文件时解密得到一个摘要,还要和从原始文件算出的另一个摘要进行比较,如果这两个摘要相同,才能打开.sig 文件,表示签名验证成功。

(3) 加密和签名

如果对文件同时进行加密和签名,需要选择对方的公钥进行加密,同时用自己的私钥对文件进行签名。

10.4.3 任务 3:使用 PGP 系统加密邮件

1. 任务目标

使用 PGP 对邮件内容进行加密、签名的操作原理和对文件的加密、签名是一样的,都是选择对方的公钥进行加密,而使用自己的私钥进行签名;对方收到后,使用自己的私钥进行

解密，而使用对方的公钥进行签名验证。

2. 工作任务

（1）加密和签名；

（2）解密和验证签名。

3. 工作环境

（1）两台预装 Windows Server 2003/XP 的主机。

（2）软件工具：PGP 加密软件。

4. 实施过程

（1）加密和签名

① 将需要加密、签名的邮件内容复制到剪贴板上，然后选择操作系统右下角 PGP 图标中的“Clipboard”→“Encrypt & Sign”命令，如图 10-20 所示。

② 在弹出的“Key Selection Dialog”对话框中，选择对方的密钥，双击使其加到下面的“Recipients”框中即可，即使用对方的公钥加密，然后单击“OK”按钮，如图 10-21 所示。

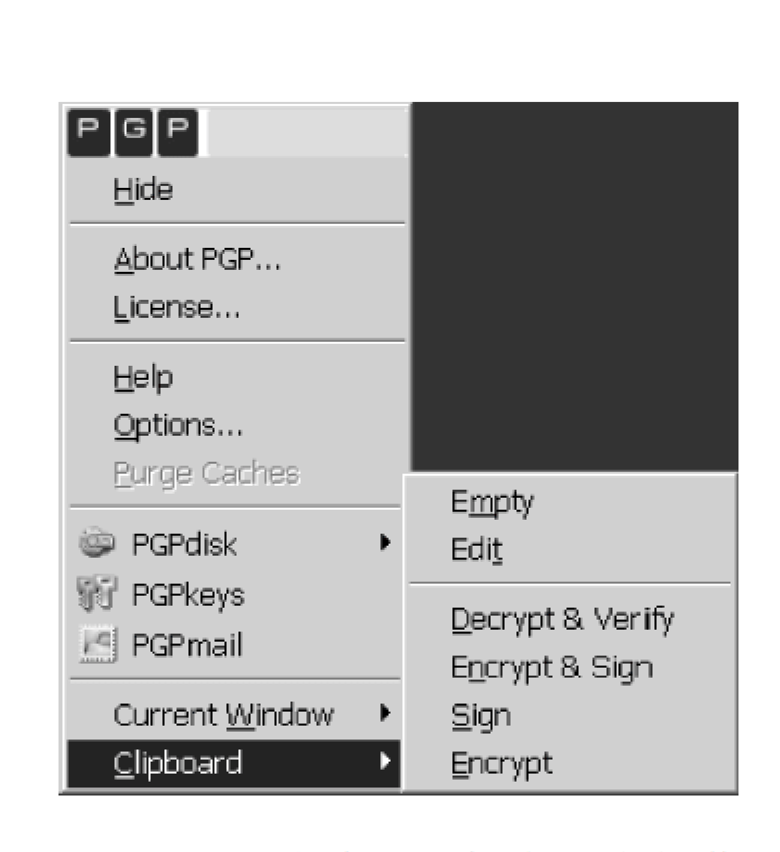


图 10-20　剪贴板的加密签名操作

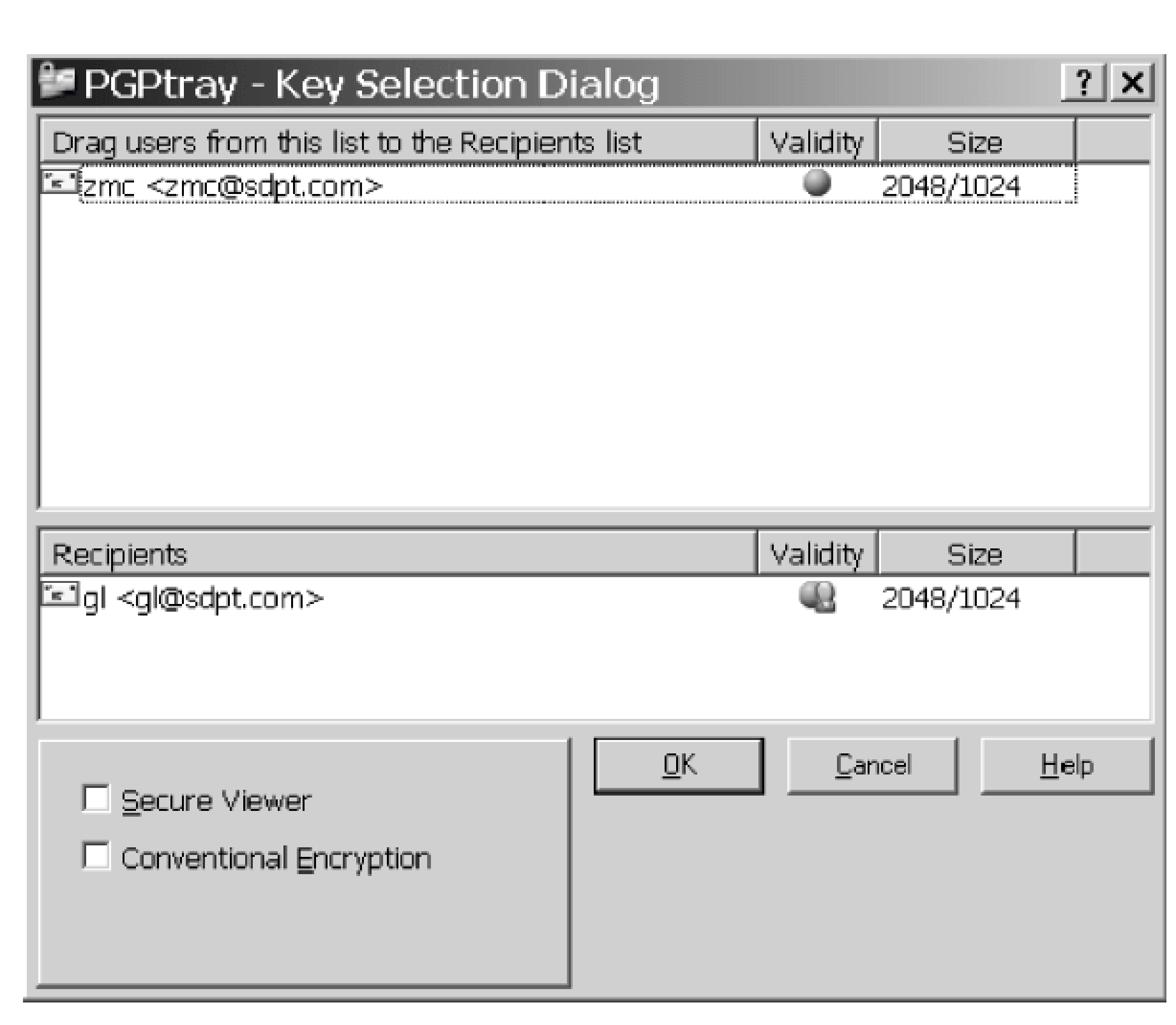


图 10-21　使用公钥加密

③ 在弹出的“Enter Passphrase”对话框中输入自己私钥的密码，进行签名，如图 10-22 所示。PGP 会将加密和签名的结果自动更新到剪贴板中。

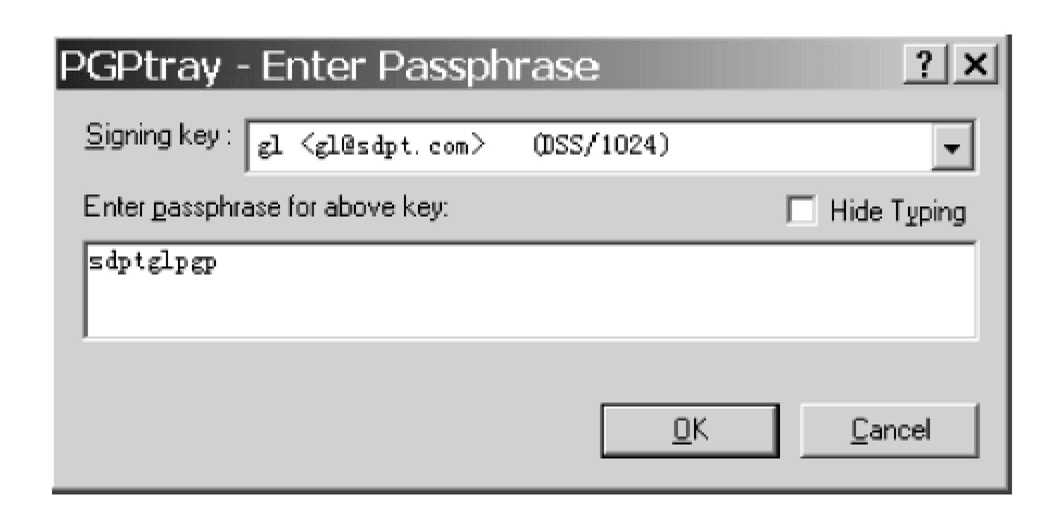


图 10-22　使用私钥的密码签名

④ 回到邮件编辑状态，只需要将剪贴板的内容粘贴过来，就会得到加密和签名后的邮件，如图 10-23 所示。



图 10-23　加密和签名后的邮件内容

（2）解密和验证签名

① 对方收到加密和签名后的邮件后，先将邮件内容复制到剪贴板中，然后选择操作系统右下角 PGP 图标中的“Clipboard”→“Decrypt & Verify”命令，将弹出输入私钥密码的提示框，如图 10-24 所示。

② 输入私钥密码进行解密和导入公钥验证签名完成后，PGP 会自动出现“Text Viewer”窗口显示结果，如图 10-25 所示。

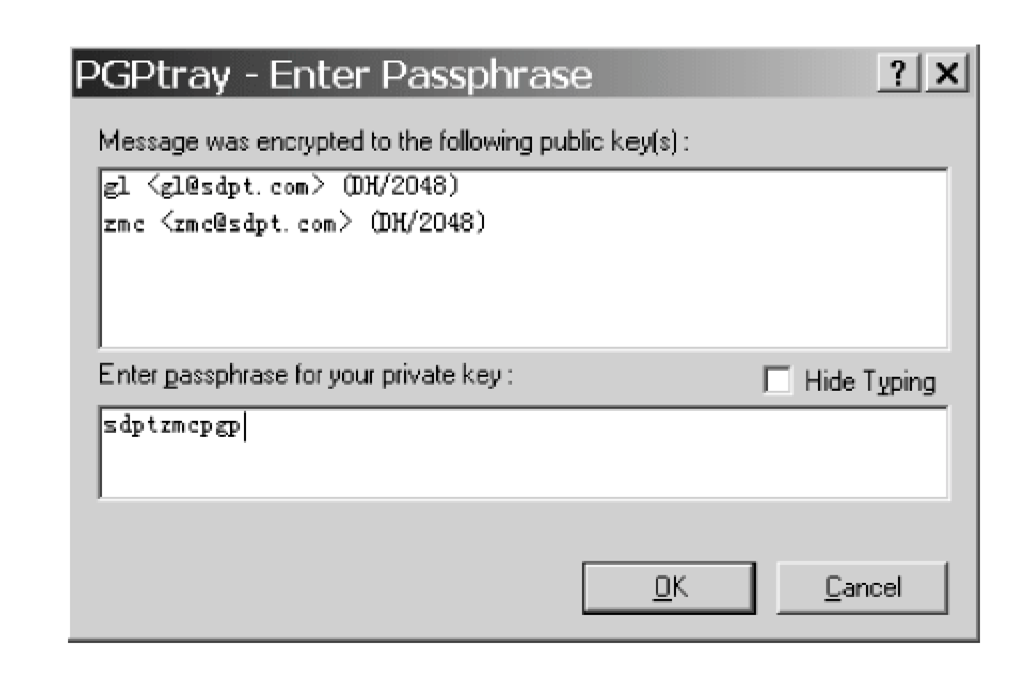



图 10-24　输入私钥密码进行解密

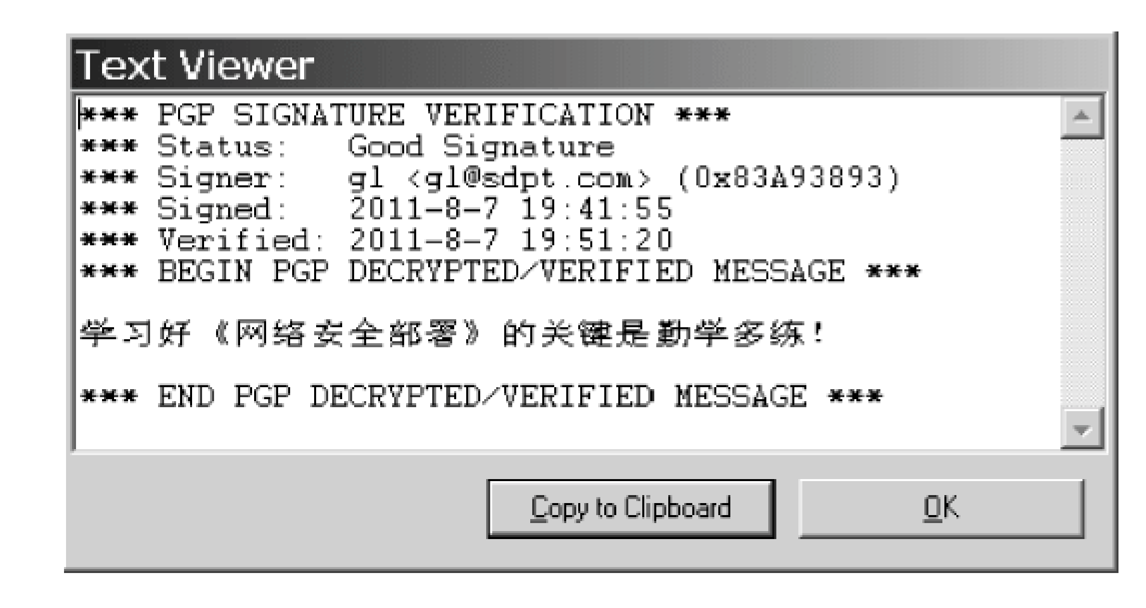


图 10-25　显示结果

单击“Copy to Clipboard”按钮，将结果复制到剪贴板中，再粘贴到需要的地方。

10.4.4　任务 4：使用 PGP 系统加密本地硬盘

1. 任务目标

PGP 加密系统不仅可以对文件、邮件加密，还可以对磁盘加密，将需要保密的数据放在

PGP加密磁盘中。即使数据硬盘被偷走，对PGP加密磁盘文件的解密也存在很大的难度，保证了数据的机密性。下面介绍使用PGP系统加密本地硬盘的方法。

2. 工作任务

(1) 创建加密磁盘；

(2) 加载加密磁盘；

(3) 卸载加密磁盘。

3. 工作环境

(1) 一台预装 Windows Server 2003/XP 的主机。

(2) 软件工具：PGP 加密软件。

4. 实施过程

(1) 创建加密磁盘

① 单击操作系统右下角的 PGP 图标，然后选择"PGPdisk"→"New Disk"命令，启动 PGP 加密磁盘创建向导，如图 10-26 所示。注意，如果 PGP 软件没有注册，无法创建加密磁盘。

② 在"PGPdisk Creation Wizard"欢迎界面中，单击"下一步"按钮，将出现如图 10-27 所示对话框，确定加密磁盘生成的路径和名称，以及加密磁盘的大小。



图 10-26　使用 PGP 构建加密磁盘

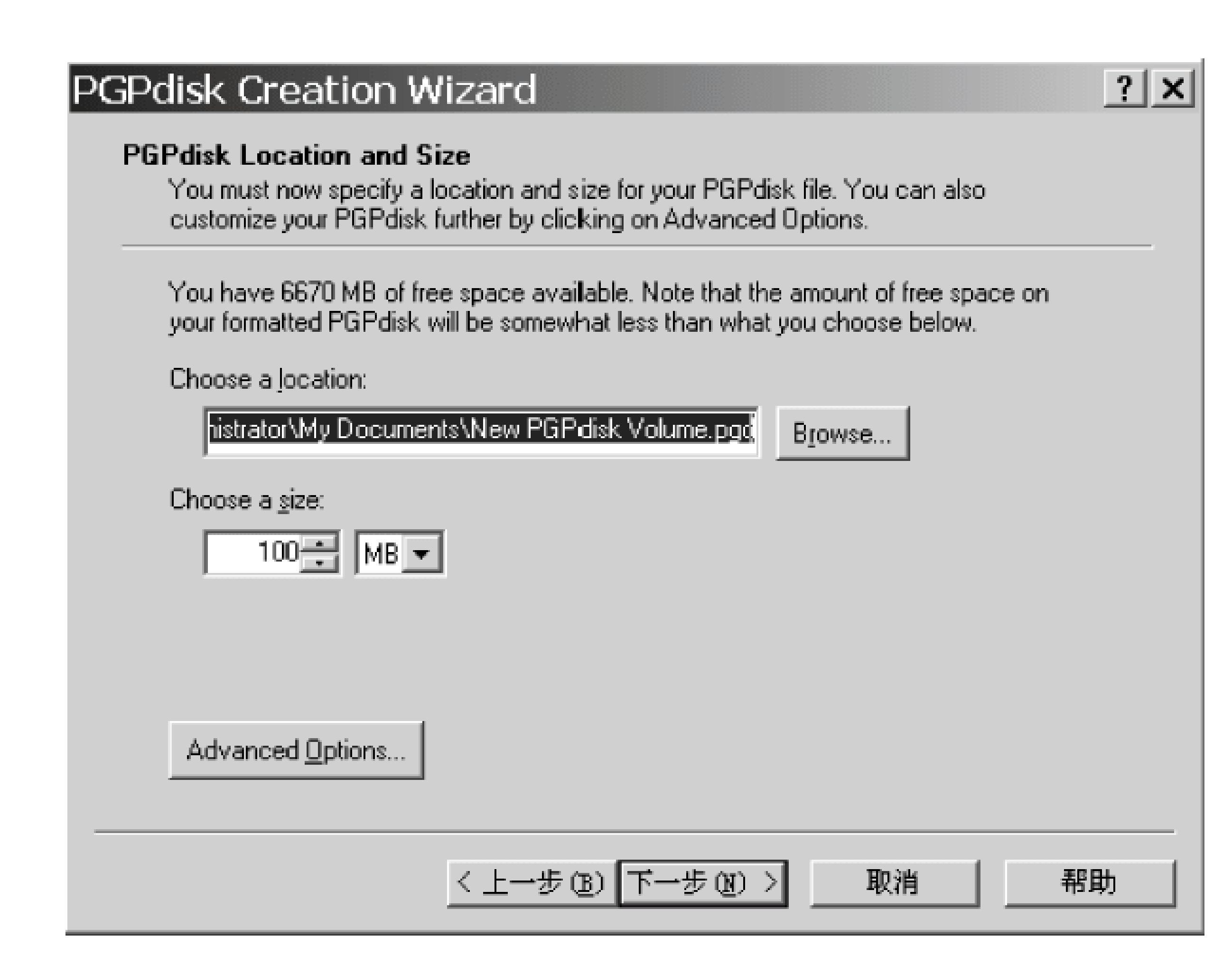


图 10-27　确定加密磁盘存放目录和大小

③ 选择加密磁盘的方法，使用公钥或者口令加密。这里选择公钥加密，如图 10-28 所示。

④ 选择一个设置好的公钥用于加密磁盘，如图 10-29 所示。

⑤ 系统需要收集一些随机数以生成密钥来加密磁盘。动一下鼠标开始收集随机数，当随机数收集至 100%时，单击"下一步"按钮。

⑥ 单击"完成"按钮，完成磁盘的创建。

(2) 加载加密磁盘

① 创建好加密磁盘后，可以在"我的电脑"中看到加密磁盘"NEW PGPDISK(E:)"，如图 10-30 所示。



图 10-28　选择使用公钥加密



图 10-29　选择加密磁盘的公钥



图 10-30　生成的加密磁盘

② 如果加密的磁盘被卸载，看不到了，可以单击操作系统右下角的 PGP 图标，选择“PGPdisk”→“Mount Disk”命令来加载磁盘，如图 10-31 所示。

③ 加载时，需要选择加载的 PGPdisk，如图 10-32 所示。





图 10-31　“PGPdisk”菜单

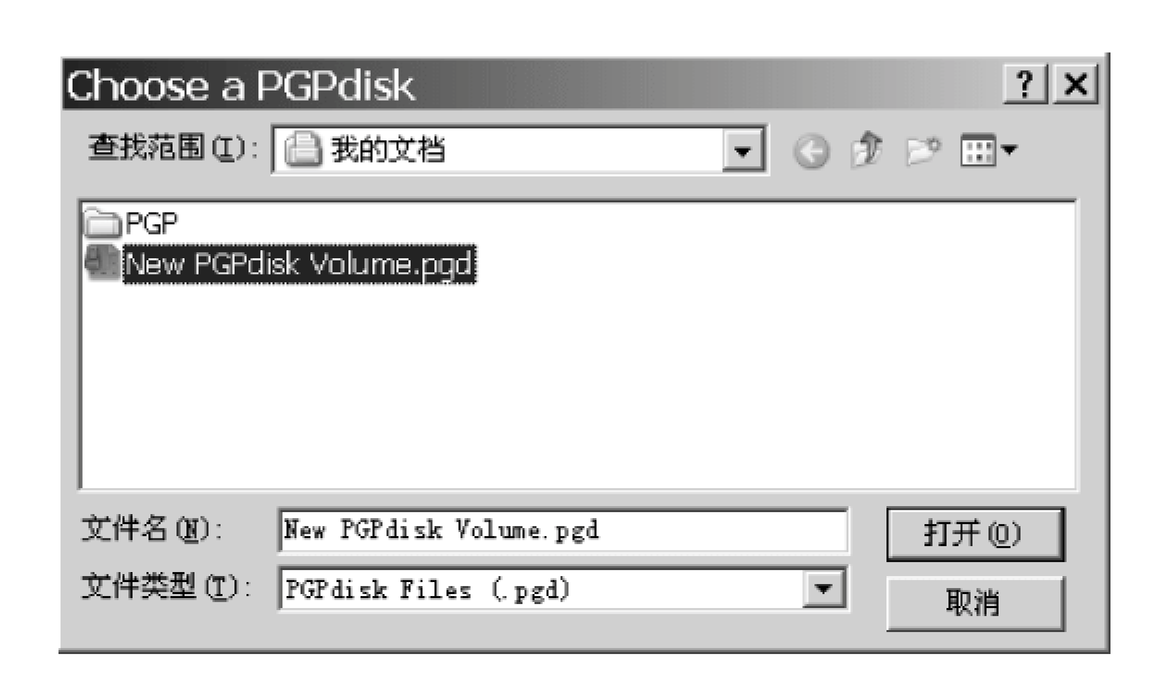


图 10-32　选择需要加载的 PGPdisk

④ 输入加密的私钥，生成加密磁盘，如图 10-33 所示。

⑤ 直接双击加密磁盘，打开加密磁盘，用户就可以把需要保密的数据放在该磁盘中，操作方法与普通磁盘一样。

(3) 卸载加密磁盘

如果暂时不需要对加密磁盘中的数据进行操作，可以卸载加密磁盘，具体步骤如下：

右击加密磁盘，在弹出的快捷菜单中选择“PGP”→“Unmount PGPdisk”命令，如图 10-34 所示。默认情况下，如果超过 15 分钟没有对加密磁盘进行操作，PGP 系统自动将加密磁盘卸载。

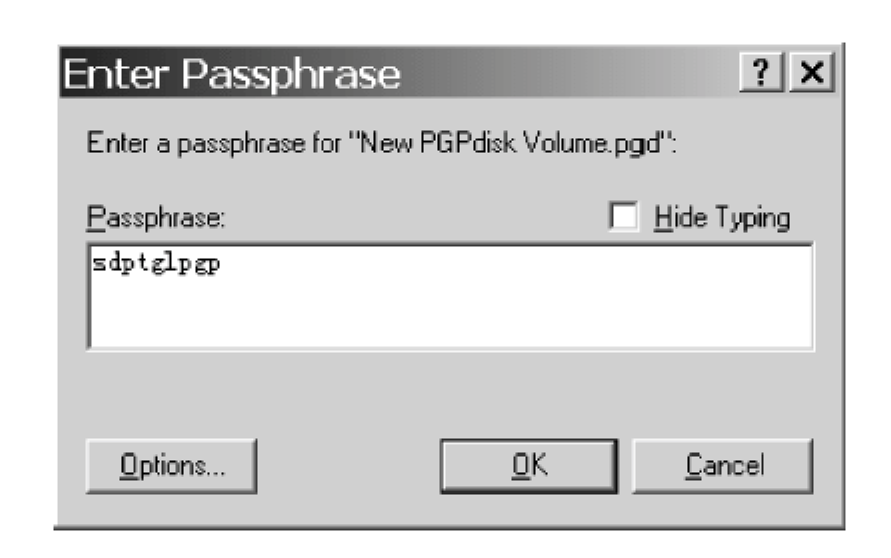


图 10-33　输入私钥的密码

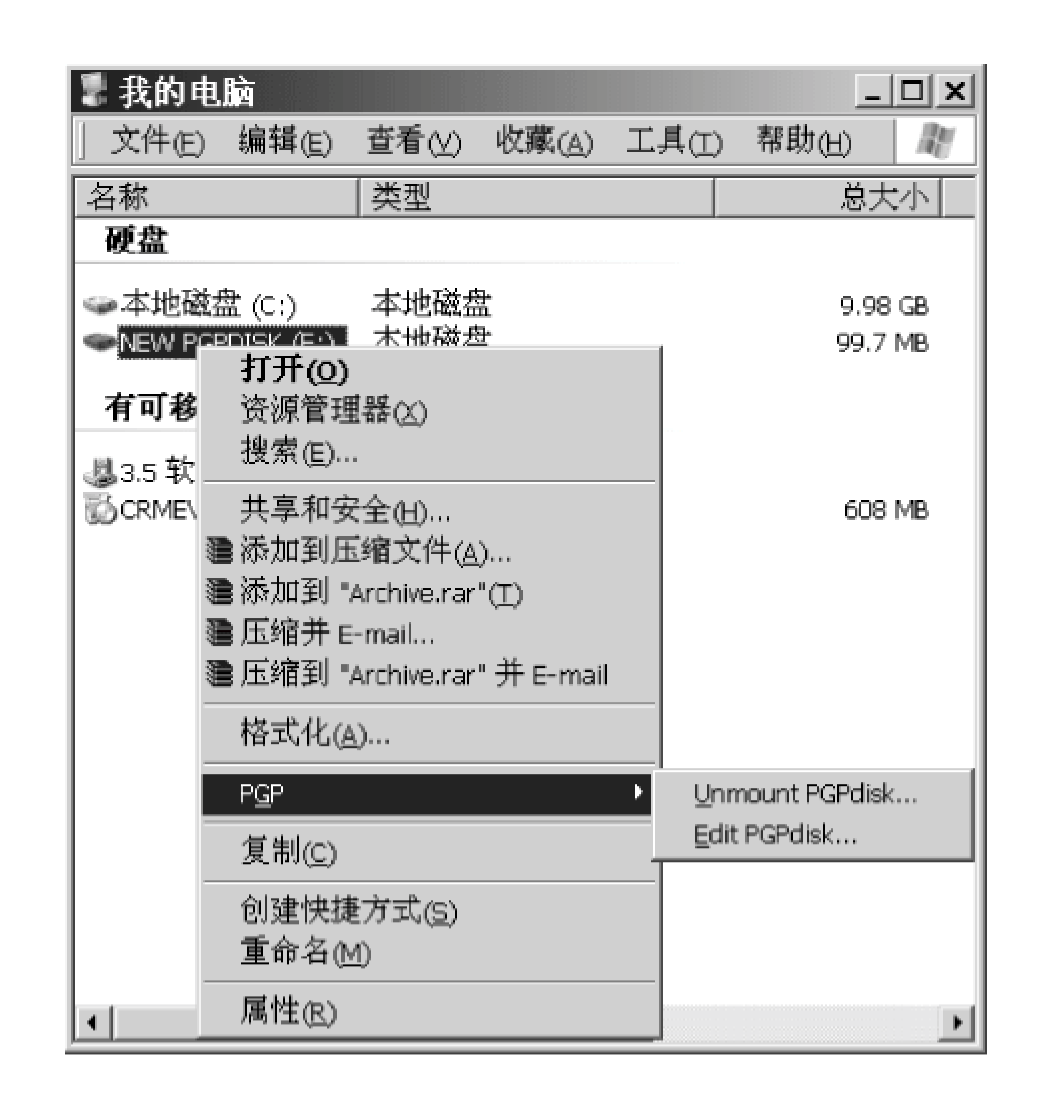


图 10-34　卸载加密磁盘

10.5　常见问题解答

若在 PGP 系统安装时，弹出如图 10-35 所示窗口，该如何处理？

答：若在双击或运行 PGP 安装程序后弹出“安装之后”对话框，那么先进行 PGP 系统

的安装，安装完毕后单击“下一步”按钮，弹出如图 10-36 所示对话框。待 PGP 系统安装结束后，再单击“完成”按钮，安装结束之前不要单击按钮。




图 10-35　“安装之后”窗口



图 10-36　“管理员安装完毕”窗口

10.6　过关练习

一、选择题

1. 数据的加密和解密是对数据进行的某种变换，加密和解密的过程都是在(　　)的控制下进行的。

A. 明文　　B. 密文　　C. 信息　　D. 密钥

2. 下面说法正确的是(　　)。

A. 信息隐蔽是加密的一种方法

B. 没有密钥，只要知道加密程序的细节就可以对信息进行解密

C. 密钥的位数越多，信息的安全性越高

D. 加密包括对称加密和非对称加密两种

3. 公开密钥算法中，加密密钥即(　　)。

A. 解密密钥　　B. 私密密钥　　C. 公开密钥　　D. 私有密钥

4. 为了防止冒名发送数据信息或发送后不承认的情况出现，采取的方法是(　　)。

A. 数字水印　　B. 数字签名　　C. 访问控制　　D. 发电子邮件确认

5. 数字签名技术在公开密钥算法中的应用是发送端采用(　　)对发送的信息进行数字签名，在接收端采用(　　)进行签名验证。

A. 发送者的公钥　　B. 发送者的私钥　　C. 接收者的公钥　　D. 接收者的私钥

6. 采用 Kerberos 系统进行认证时，可以在报文中加入 (　　)来防止重放攻击。

A. 会话密钥　　B. 时间戳　　C. 用户 ID　　D. 私有密钥

7. DES 是一种(　　)算法。

A. 共享密钥　　B. 公开密钥　　C. 报文摘要　　D. 访问控制

8. 安全电子邮件协议 PGP 不支持(　　)。

A. 确认发送者的身份　　B. 确认电子邮件未被修改

C. 防止非授权者阅读电子邮件　　D. 压缩电子邮件大小

二、填空题

1. 现实中通常将对称加密算法和非对称加密算法混合起来使用，使用________算法对要发送的数据进行加密，其密钥使用________算法进行加密，以综合发挥两种加密算法的优点。

2. PGP加密系统不仅可以对文件数据进行加密，还可以对________、________等进行加密。

三、简答题

1. 简述DES算法的基本思想。

2. 使用PGP加密系统对文件进行签名后，将签名后的.sig文件发送给对方的同时，为什么还要发送原始文件给对方？

四、实操题

1. 利用PGP加密系统加密邮件。

2. 利用PGP加密系统进行签名和验证操作。

工作任务十一

Internet信息服务的安全设置

11.1　用户需求与分析

Internet 信息服务即 IIS，是一个用于配置应用程序池或网站、FTP 站点、SMTP 或 NNTP 站点的工具。利用 IIS 管理器，网络安全管理员可以配置 IIS 安全、性能和可靠性功能，可添加或删除站点，启动、停止和暂停站点，备份和还原服务器配置，创建虚拟目录以改善内容管理等。正是因为 IIS 具有如此强大的功能，其安全问题更加受到人们的重视，并需要设置 IIS 的安全来保护系统中的数据。

11.2　预 备 知 识

11.2.1　Web 的安全问题

Web 服务是常用的网络服务之一，通过 IIS 可以搭建信息发布、信息查询、电子商务、电子政务等各种用途的 Web 网站。Web 站点的基本配置及其含义如表 11-1 所示。

表 11-1　Web 站点的基本配置

选项组	配　置　项	说　　明
Web 站点标识	说明	显示在 IIS 控制台的名称，以区别各个站点
	IP 地址	Web 服务器对外服务的 IP 地址
	TCP 端口	Web 服务器服务的 TCP 端口号，默认为 80。若更改，访问时必须在 URL 中指出
	SSL 端口号	使用安全套接字访问(用 https://)的端口号，默认为 443
	“高级”按钮	除修改 IP 地址、端口号外，还可修改站点的主机头
连接	无限	对同时连接站点的用户数不做限制
	限制	根据实际情况限制同时连接站点的用户数量
	连接超时	如果用户在规定的时间内没有和 Web 服务器进行信息交换，则自动中断此用户的连接
	启用保持 HTTP 激活	允许客户端保持与服务器的开放连接
日志	启用日志记录	日志用来记录服务器的访问、错误等信息，需要设置日志格式、日志记录内容和记录方法等

另外，许多基于 Web 管理界面的其他网络服务同样需要用到 Web 服务器的安全，例如邮件服务器、流媒体服务器等。因此，Web 服务器的安全性将影响到本地系统，甚至整个网

络的安全性,必须通过相应的安全机制控制来访用户的访问。

可以通过验证 Web 站点的 CA 数字证书来判别该站点的真伪。Web 流量安全在网络级的解决方法之一是使用 IPSec,在传输级的解决方法之一是使用安全套接层(SSL)或传输层安全(TLS),在应用级的解决方法之一是使用安全的电子交易(SET)。Web 站点的四级访问控制是 IP 地址限制、用户验证、Web 权限、NTFS 权限。IE 的四个区域分别是 Internet 区域、本地 Intranet 区域、可信站点区域和受限站点区域。

安全套接层(SSL)位于 HTTP 层和 TCP 层之间,建立客户机与服务器之间的加密通信,以确保 HTTP、FTP、SMTP、POP3、Telnet 等服务信息传递的安全性。SSL 协议包括 SSL 记录协议和 SSL 握手协议两个子协议。其中,记录协议位于握手协议之下,主要为 SSL 连接提供机密性和报文完整性服务。SSL 握手协议被封装在 SSL 记录协议中,它允许服务器与客户机在应用程序传输和接收数据之前互相认证、协商加密算法(RSA、DH 等)和密钥。密钥协商使用非对称(公钥)密钥体制进行。

在 IIS 6.0 中,Web 服务器管理员必须首先安装 Web 站点数字证书,Web 服务器才能支持 SSL 会晤。数字证书的格式遵循 ITU-T X.509 标准。通常情况下,数字证书需要由证书认证机构(CA)颁发。

11.2.2　FTP 的安全问题

FTP 服务主要用于实现在 FTP 服务器和 FTP 客户端之间传输文件。通过 FTP 服务,可以实现软件的下载,文件的交换与共享,以及 Web 站点的维护。很多网络管理员或者安全工程师在维护服务器时所使用的 FTP 系统在工作中非常重要,但是一般都不公开或者很少公开,所以安全性往往得不到足够的重视,成为很多攻击者喜欢攻击的目标。

11.3　方 案 设 计

方案设计如表 11-2 所示。

表 11-2　方案设计

任务名称	Internet 信息服务的安全设置
任务分解	1. Web 服务器的安全设置 (1) 用户身份认证 (2) IP 地址限制 (3) 端口安全 (4) 为 Web 站点启用 SSL 安全保护 2. 构建高安全性的 FTP 服务器 (1) 指定 FTP 的 IP 地址并修改默认端口 (2) 定制详细的 FTP 日志,记录相关信息 (3) 利用 NTFS 约束 FTP 用户权限 (4) 启用目录安全性,杜绝 99%的各类 FTP 攻击

续表

能力目标	1. 能设置 Web 服务器的“用户身份认证”访问方式 2. 能通过 IP 地址限制进行 Web 服务器的身份认证 3. 能为 Web 站点启用 SSL 安全保护 4. 能修改 FTP 的 IP 地址和默认端口 5. 能定制详细的 FTP 日志，记录相关信息 6. 能利用 NTFS 约束 FTP 用户权限 7. 能启用目录安全性，杜绝各类 FTP 攻击
知识目标	1. 了解 Web 服务器的安全问题 2. 了解 FTP 服务器的安全问题
素质目标	1. 树立较强的安全意识 2. 掌握网络安全行业的基本情况 3. 培养职业兴趣，以及爱岗敬业、热情主动的工作态度 4. 培养良好的职业道德 5. 具有可持续发展能力

11.4 任务实施

11.4.1 任务 1：Web 服务器的安全设置

1. 任务目标

Web 服务已经成为众多网络的必备服务，被用来提供信息发布、邮件查询、电子商务、网络办公等网络平台。但是，一般用户都是在对 Web 安全了解甚少的情况下使用的，Web 服务的安全直接决定多种网络服务的安全，涉及整个网络的安全，因此本任务通过对 Web 服务器的简单配置，获得安全、可靠的网络平台。

2. 工作任务

(1) 用户身份认证；

(2) IP 地址限制；

(3) 端口安全；

(4) 为 Web 站点启用 SSL 安全保护。

3. 工作环境

三台预装 Web 服务器的 Windows Server 2003/XP 主机。

4. 实施过程

(1) 用户身份认证

由 IIS 搭建的 Web 网站默认所有用户匿名访问，网络中的用户无须输入用户名和密码就可以任意访问 Web 网页。但对于一些安全性要求较高的 Web 网站，或者 Web 网站中拥有敏感信息时，可以采用用户认证的方式，确保只有经过授权的用户才可以对 Web 信息进行访问和浏览。具体的实现步骤如下：

① 启动 IIS，打开“默认网站 属性”对话框，然后选择“目录安全性”选项卡，如图 11-1 所示。

② 单击“编辑”按钮，打开“身份验证方法”对话框。撤选“启用匿名访问”，取消 Web 站点的匿名访问服务，然后选择“集成 Windows 身份验证”，单击“确定”按钮，如图 11-2 所示。

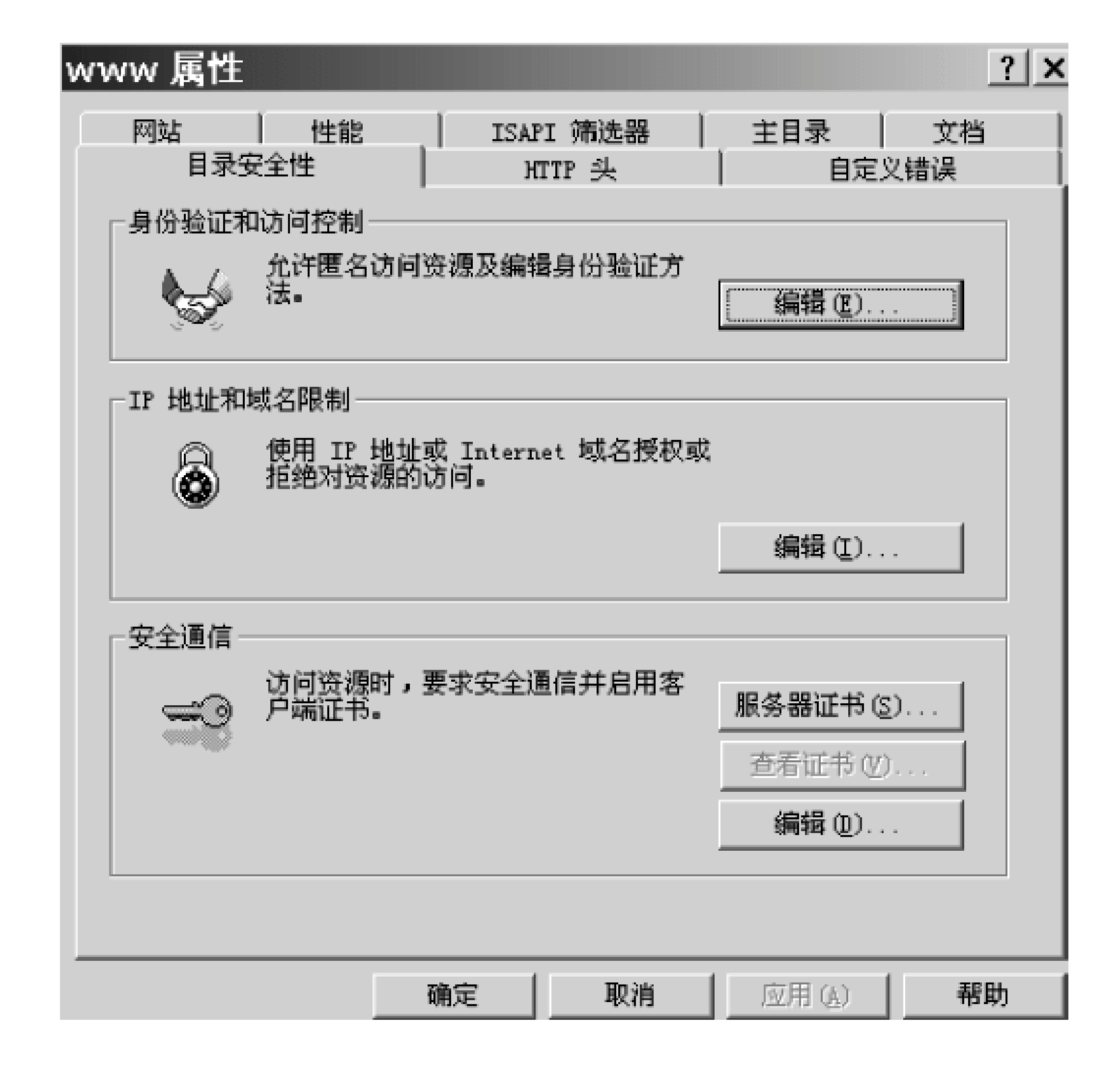


图 11-1　网站属性“目录安全性”选项卡

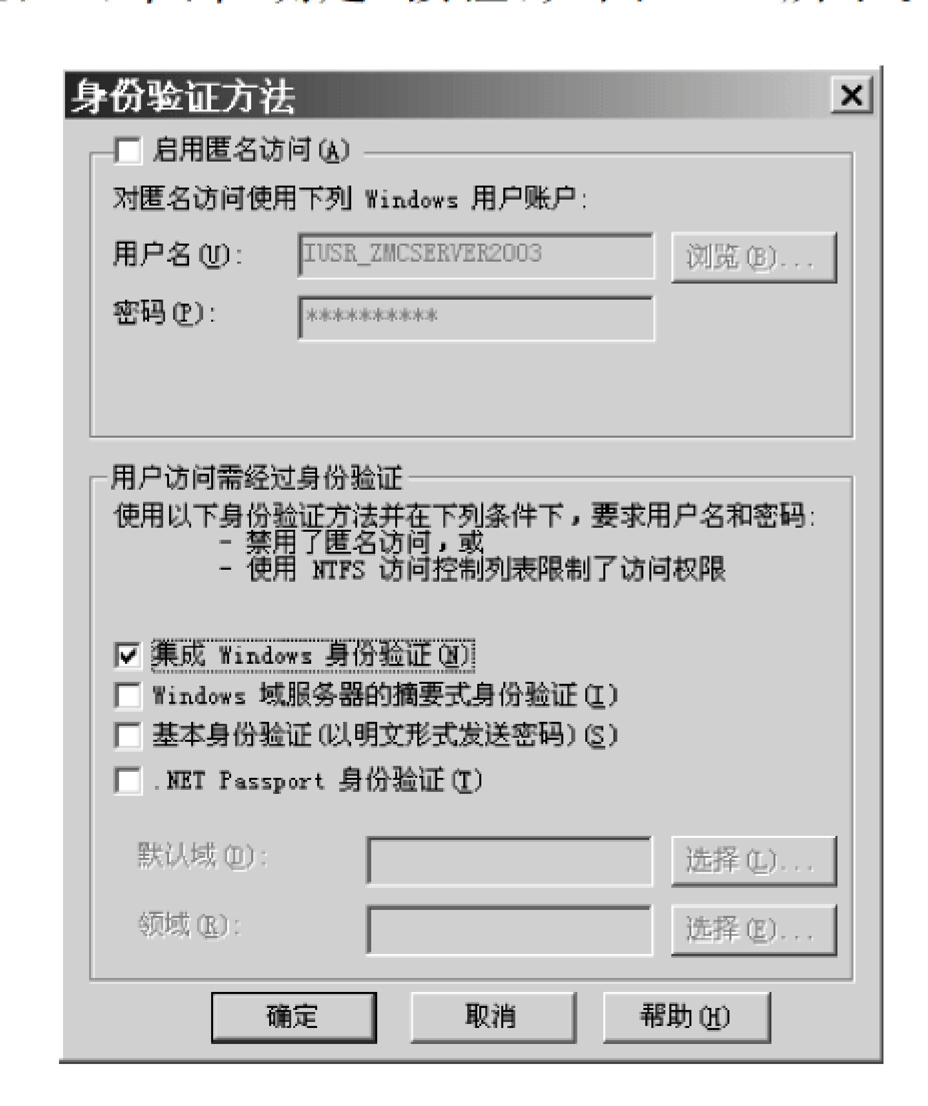


图 11-2　“身份验证方法”对话框

“集成 Windows 身份验证”是一种安全的验证形式，需要用户输入用户名和密码，因为用户名和密码在通过网络发送前会经过散列处理，因此可以确保安全性。它是 Windows Server 2003 家族成员中使用的默认身份验证方式，安全性较高。

③ 访问 Web 站点，将弹出登录对话框，需要输入正确的用户名和密码才能打开网页，如图 11-3 所示。

把 Web 服务器安装在系统的 NTFS 分区上，可以对 NTFS 文件系统的文件和文件夹的访问权限进行控制，对不同的用户和用户组授予不同的访问权限。具体的实现步骤如下：

① 选择要设定访问权限的文件或文件夹，然后右击选择快捷菜单中的“共享和安全”菜单项，在打开的属性对话框中选择“安全”选项卡，如图 11-4 所示。



图 11-3　登录对话框



图 11-4　“安全”选项卡(1)

② 设置允许访问该文件夹的不同用户和组的权限。例如，可以把其他组和用户都删掉，只添加一个用户 web01 对 Web 服务器的文件夹具有读取和运行、列出文件夹目录以及读取和写入的权限，如图 11-5 所示，则其他组或用户都不能访问该文件夹。

对于已经设置成 Web 目录的文件夹，可以通过操作站点属性实现对 Web 目录访问权限的控制，具体实现方法如下：在 IIS 中打开站点的属性对话框，然后选择“主目录”选项卡，设置 Web 目录的访问权限，如图 11-6 所示。

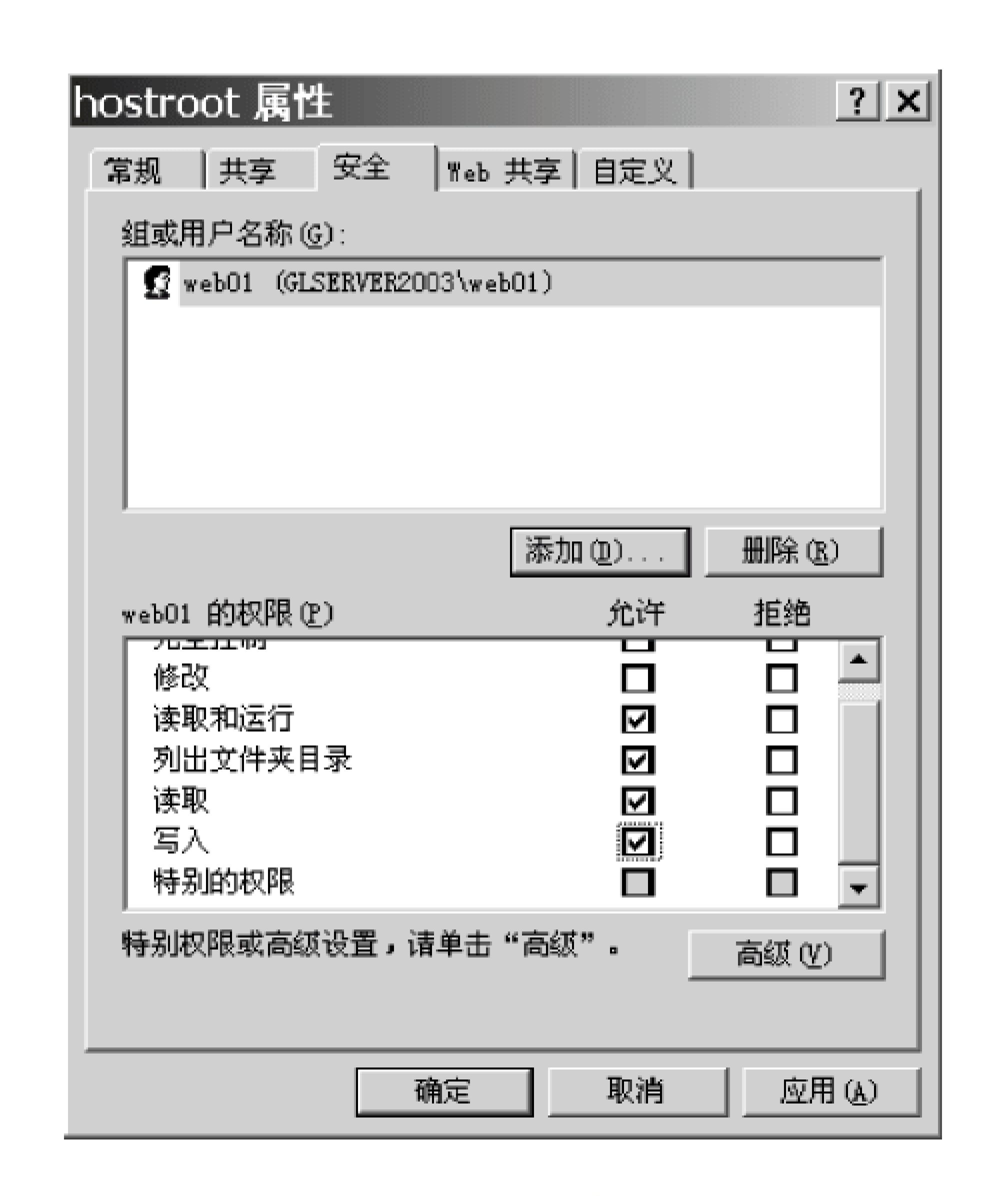


图 11-5 设置用户和权限

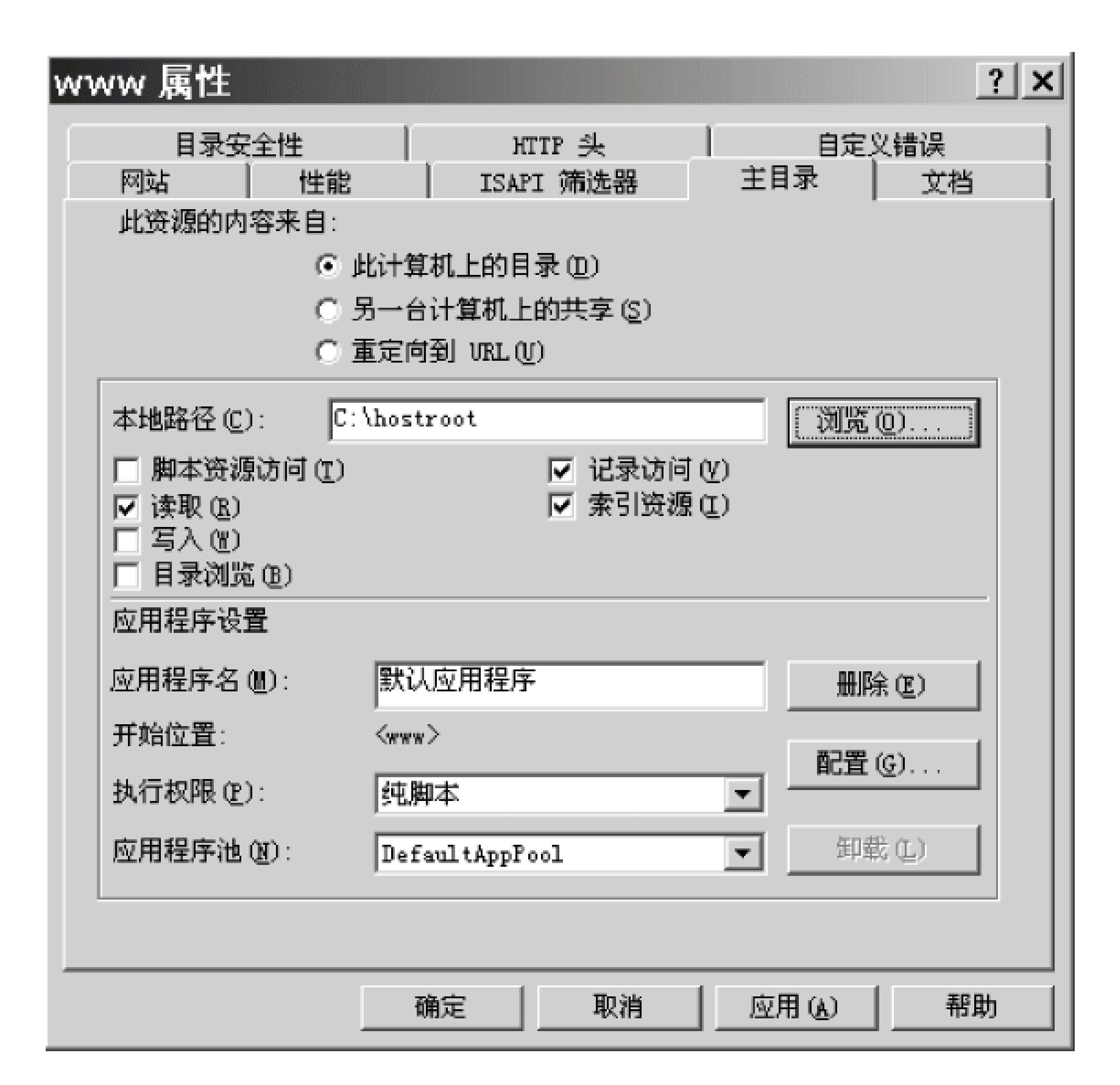


图 11-6 “主目录”选项卡(1)

注意：“脚本资源访问”权限的设定可能给其他人利用 ASP 脚本漏洞对 Web 网站发动恶意攻击，或暴露数据库的位置，一般不予选中。“读取”权限允许用户读取或下载文件或目录及其相关属性，如果要发布信息，必须选中。“写入”权限允许用户将文件上传到 Web 服务器上已启用的目录中，或者更改可写文件的内容，仅仅发布信息，不用选中。当允许用户“写入”时，一定要选择相应的用户身份验证方式，并设置磁盘配额，防止非法用户入侵，以及授权用户对磁盘空间的滥用。“目录浏览”权限允许客户看到该虚拟目录下的文件和子目录的超文本列表，从而容易导致对网站的恶意攻击，一般不选中。“记录访问”权限可以对 Web 网站的访问进行统计和分析，有益于系统安全，但要同时启用该网站的日志记录，才有访问记录。“索引资源”权限允许 Microsoft Indexing Service 将该目录包含在 Web 网站的全文索引中。

(2) IP 地址限制

使用用户身份认证方式后，每次访问 Web 站点都需要输入用户名和密码，这对于授权用户来说非常麻烦，可以通过 IP 地址限制来进行身份认证，简单且有效。可以把 Web 站点设置成允许或拒绝从特定 IP 发来的服务请求，有选择地允许特定用户访问 Web 服务，拒绝除了特定 IP 地址外的整个网络用户来访问 Web 服务器。具体操作步骤如下：

① 打开 Web 站点属性对话框，选择“目录安全性”选项卡，然后单击“IP 地址和域名限制”选项区域的“编辑”按钮，打开“IP 地址和域名限制”对话框，如图 11-7 所示。

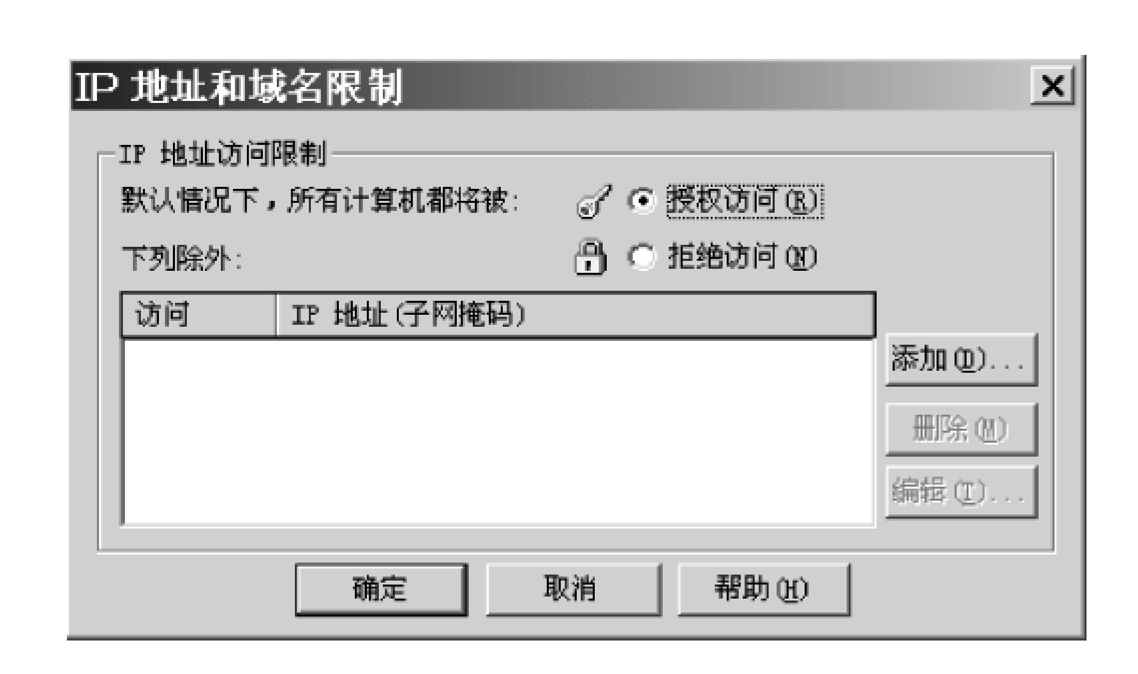


图 11-7 “IP 地址和域名限制”对话框

② 选中“授权访问”选项，然后单击“添加”按钮，有三种方式来限制连接。

• 选择“一台计算机”，利用 IP 地址拒绝某台计算机访问 Web 网站，如图 11-8 所示。

• 选择“一组计算机”，利用“网络标识”和“子网掩码”来拒绝某一个网段内的所有计算机访问 Web 网站，如图 11-9 所示。



图 11-8 拒绝一台计算机访问

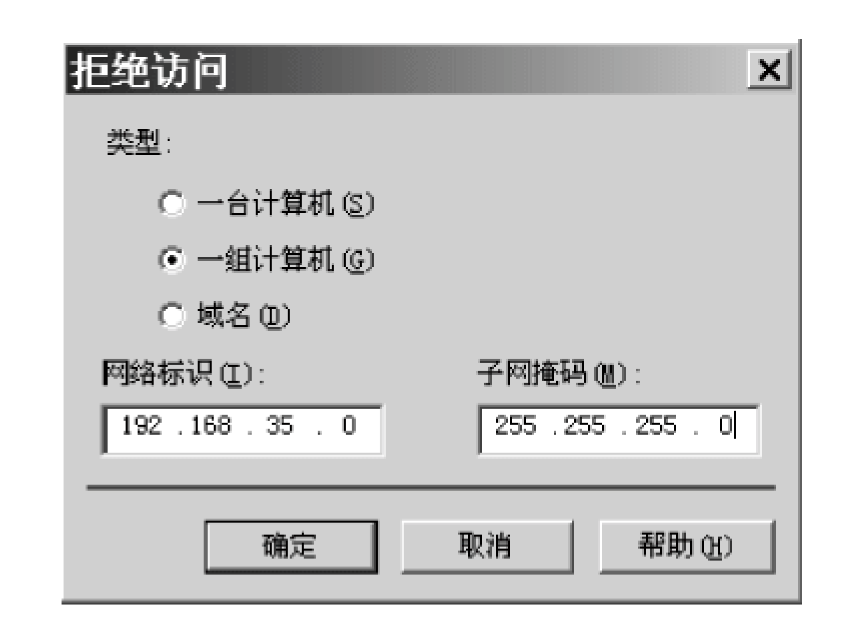


图 11-9 拒绝一组计算机访问

• 选择“域名”，利用计算机域名来拒绝某台计算机访问 Web 网站，如图 11-10 所示。

③ 选择完毕后，单击“确定”按钮，所有被拒绝的计算机访问该网站时，都会显示如图 11-11 所示的“您未被授权查看该页”的提示。

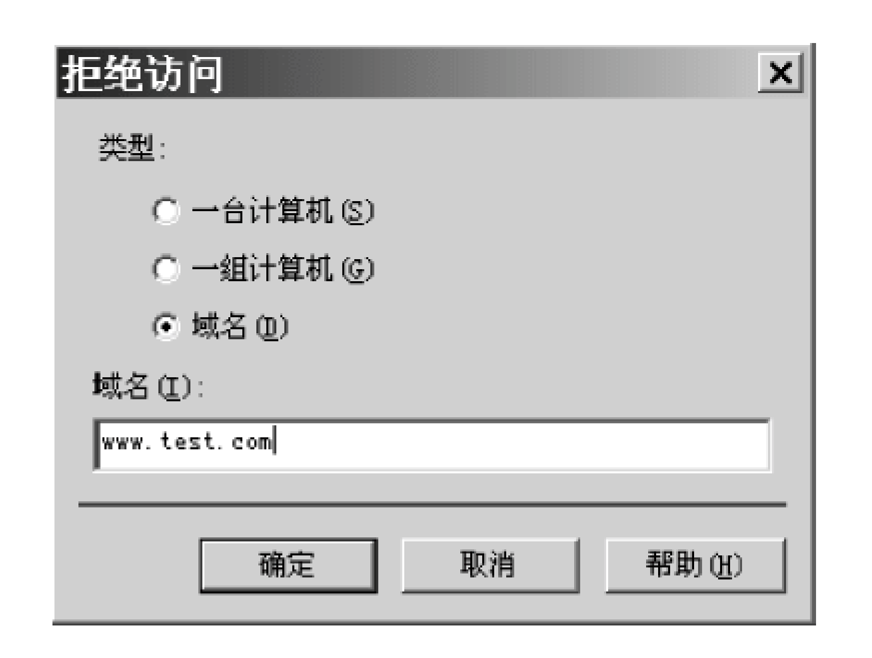


图 11-10 根据域名拒绝一台计算机访问

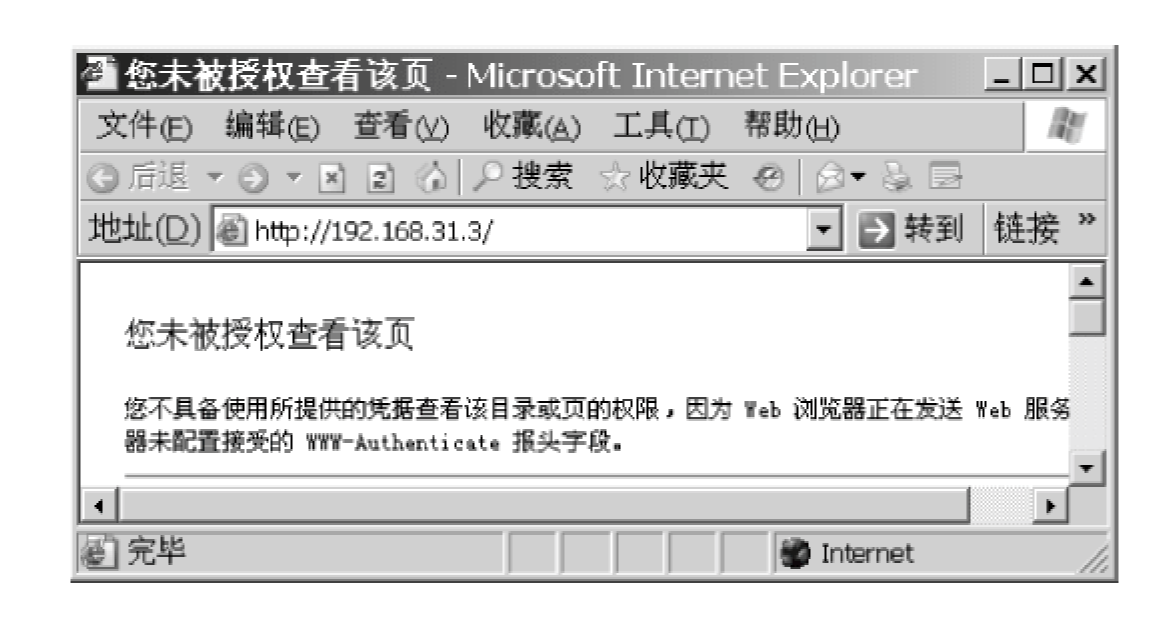


图 11-11 网站拒绝访问提示

如果单击“拒绝访问”选项，则与“授权访问”选项刚好相反；单击“添加”按钮，会打开“授权访问”对话框，用来添加特别授予访问权限的计算机。

(3) 端口安全

Web 站点的 TCP 端口默认是 80，可以通过修改默认端口号来提高 Web 服务的安全

性。但如果修改了端口号，就只有知道端口号的用户才能访问企业 Web 站点。修改端口号的方法是打开站点的属性对话框，然后选择“网站”选项卡，在其中输入新的 TCP 端口号，如图 11-12 所示。

图 11-12 端口设置

（4）为 Web 站点启用 SSL 安全保护

SSL(Secure Socket Layer)又称为 TLS 协议，是 Netscape 研制开发的，用以保障在互联网上的数据传输安全。它利用数据加密技术，避免数据被中途截获和篡改。HTTP 协议可以用 SSL 来加密传输安全性较高的数据和信息，达到安全传输的目的。

本任务使用三台计算机，一台作为企业 Web 服务器，一台作为客户机，一台作为证书颁发机构 CA。客户机通过 IE 浏览器访问企业 Web 站点。企业 Web 服务器通过向证书颁发机构 CA 申请并安装服务器证书，并要求客户机通过 SSL 安全通道连接，保证双方通信的机密性、完整性和服务器的用户身份认证。同时，通过在客户机上申请并安装客户端证书，实现客户机的用户身份认证。

这里说的证书全称为数字证书，是一种由证书颁发机构颁发并经证书颁发机构数字签名的、用于证明证书持有人身份的“网络身份证”，其中包括了证书持有人的公钥信息和证书颁发机构的数字签名，还可以包括用户的其他信息。数字证书的权威性取决于证书颁发机构的权威性。

首先，在一台计算机上安装“证书服务”组件，使之成为一个证书颁发机构 CA，具体的实现步骤如下：

① 单击“开始”→“控制面板”→“添加删除 Windows 组件”→“证书服务”，提示安装“证书服务”后就不能改变计算机名了，然后单击“是”按钮，如图 11-13 所示。

② 单击“下一步”按钮，弹出“CA 类型”对话框，有四种类型的证书颁发机构。如果本机是活动目录，则都可以选；如果不是，只能选择后两项，即“独立根 CA”(CA 体系中最受信任的 CA，不需要 Active Directory)和“独立从属 CA”(标准 CA，可以给任何用户或计算机颁

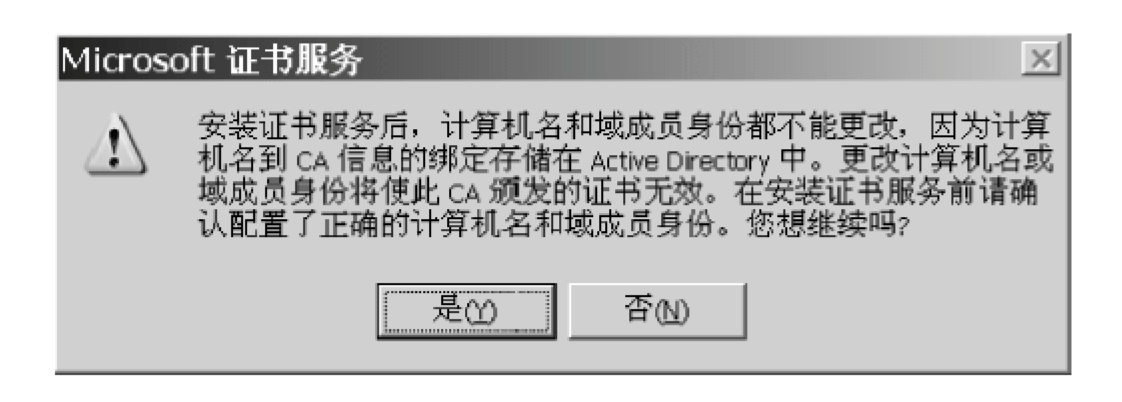


图 11-13　提示信息

发证书，但必须从另一个 CA 获取 CA 证书，不需要 Active Directory）。这里选择“独立根 CA”，如图 11-14 所示。

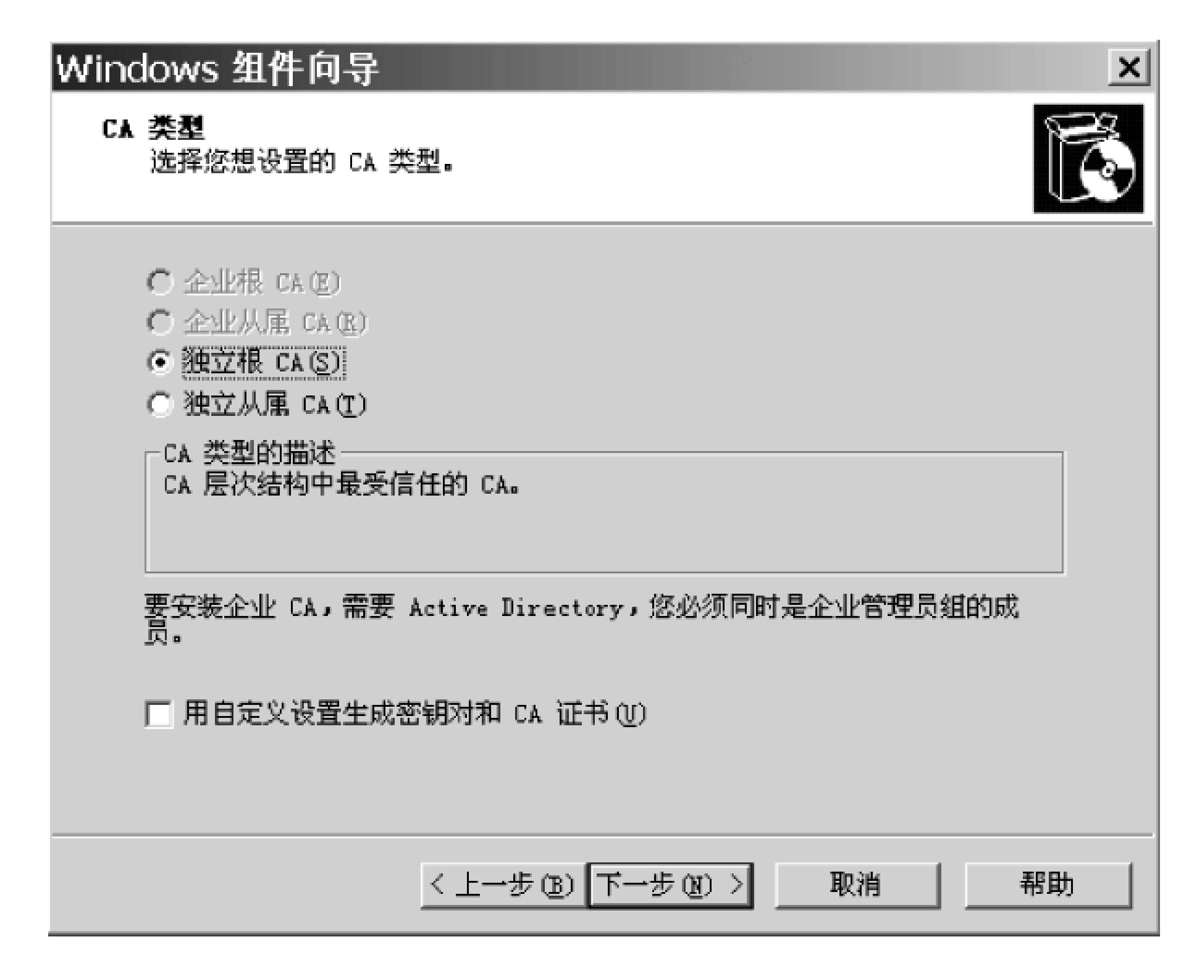


图 11-14　“CA 类型”对话框

③ 单击“下一步”按钮，弹出“CA 识别信息”对话框。为安装的 CA 起一个公用名称，“可分辨名称后缀”可以不填，“有效期限”默认为 5 年，如图 11-15 所示。



图 11-15　“CA 识别信息”对话框

④ 单击“下一步”按钮，弹出“证书数据库设置”对话框，显示证书数据库与日志存放位置的设置，默认为 C:\WINDOWS\system32\CertLog，如图 11-16 所示。这里保持默认设置，因为只有这样，系统才会根据证书类型自动分类和调用。



图 11-16 “证书数据库设置”对话框

⑤ 配置好参数后，系统开始安装证书服务组件，要求有系统 I386 安装文件。指定好位置后，开始 CA 服务的安装。

⑥ 在安装过程中弹出“是否启用 Active Server Page”对话框，单击“是”按钮，完成证书服务，如图 11-17 所示。

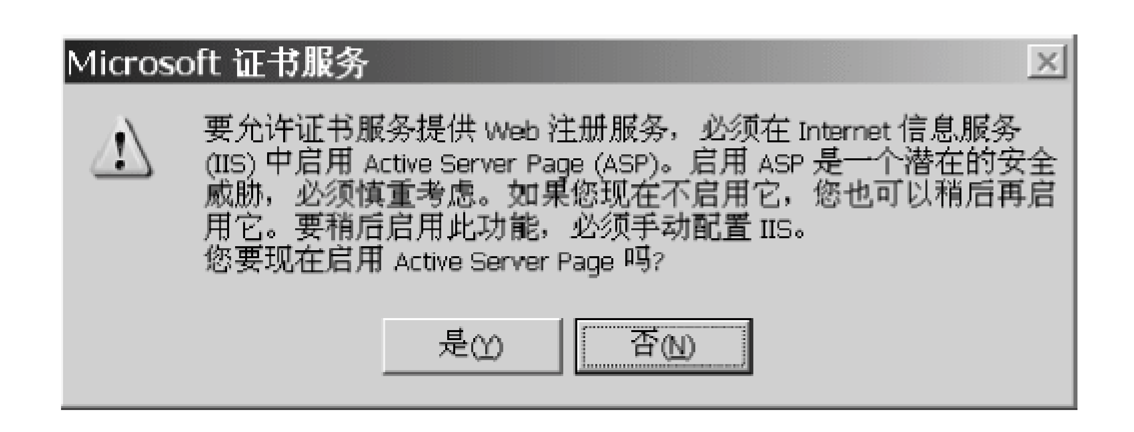


图 11-17 “是否启用 Active Server Page”对话框

然后，在企业 Web 服务器上创建证书请求文件，这需要通过 IIS 以 Web 形式完成，具体的操作如下：

① 选择 IIS 中企业 Web 站点的“目录安全性”选项卡，然后单击“安全通信”选项区域的“服务器证书”按钮，打开 Web 服务器证书向导。

② 单击“下一步”按钮，弹出“服务器证书”对话框，选中“新建证书”选项，如图 11-18 所示。

③ 单击“下一步”按钮，弹出“延迟或立即请求”对话框，选择“现在准备证书请求，但稍后发送”。然后单击“下一步”按钮，弹出“名称和安全性设置”对话框，设置新证书的名称和密钥长度，如图 11-19 所示。

④ 单击“下一步”按钮，弹出“单位信息”对话框，设置证书所包含单位的相关信息，以便和其他单位的证书区分开，如图 11-20 所示。

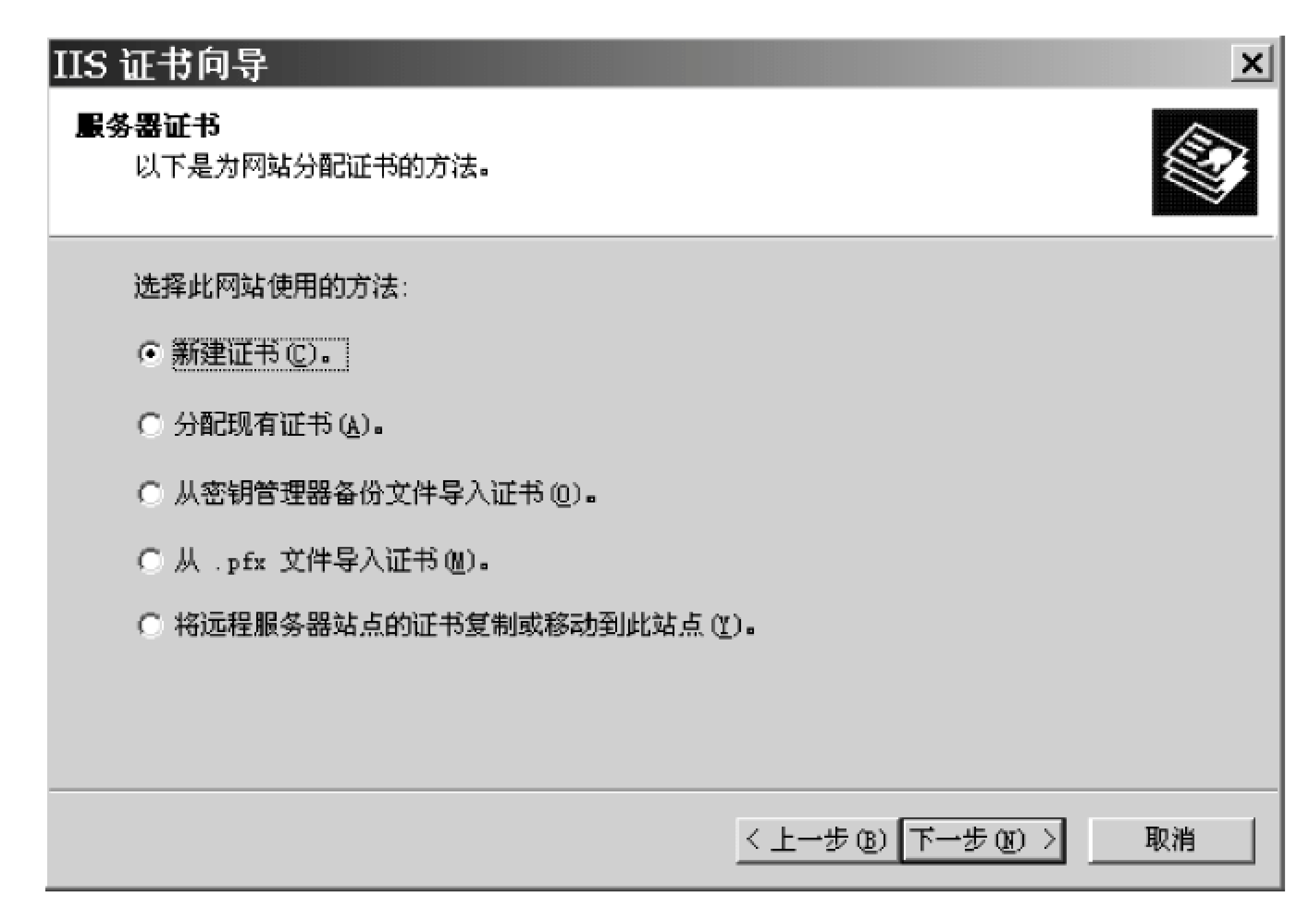


图 11-18　“服务器证书”对话框

IIS 证书向导

名称和安全性设置

新证书必须具有名称和特定的位长。

输入新证书的名称。此名称应易于引用和记忆。

名称(M):

www

密钥的位长决定了证书的加密程度。位长越长，安全性越高。然而，位长过长将使性能降低。

位长(H): 1024

选择证书的加密服务提供程序(CSP)(P)

< 上一步(B)　下一步(N) >　取消

图 11-19　“名称和安全性设置”对话框

IIS 证书向导

单位信息

证书必须包含您单位的相关信息，以便与其他单位的证书区分开。

选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。

如需详细信息，请参阅证书颁发机构的网站。

单位(O):

sdpt

部门(U):

computer

< 上一步(B)　下一步(N) >　取消

图 11-20　“单位信息”对话框

⑤ 单击“下一步”按钮,弹出“站点公用名称”对话框。如果服务器在互联网上,需填写有效的域名;如果服务器在局域网内,需填写计算机名,如图 11-21 所示。

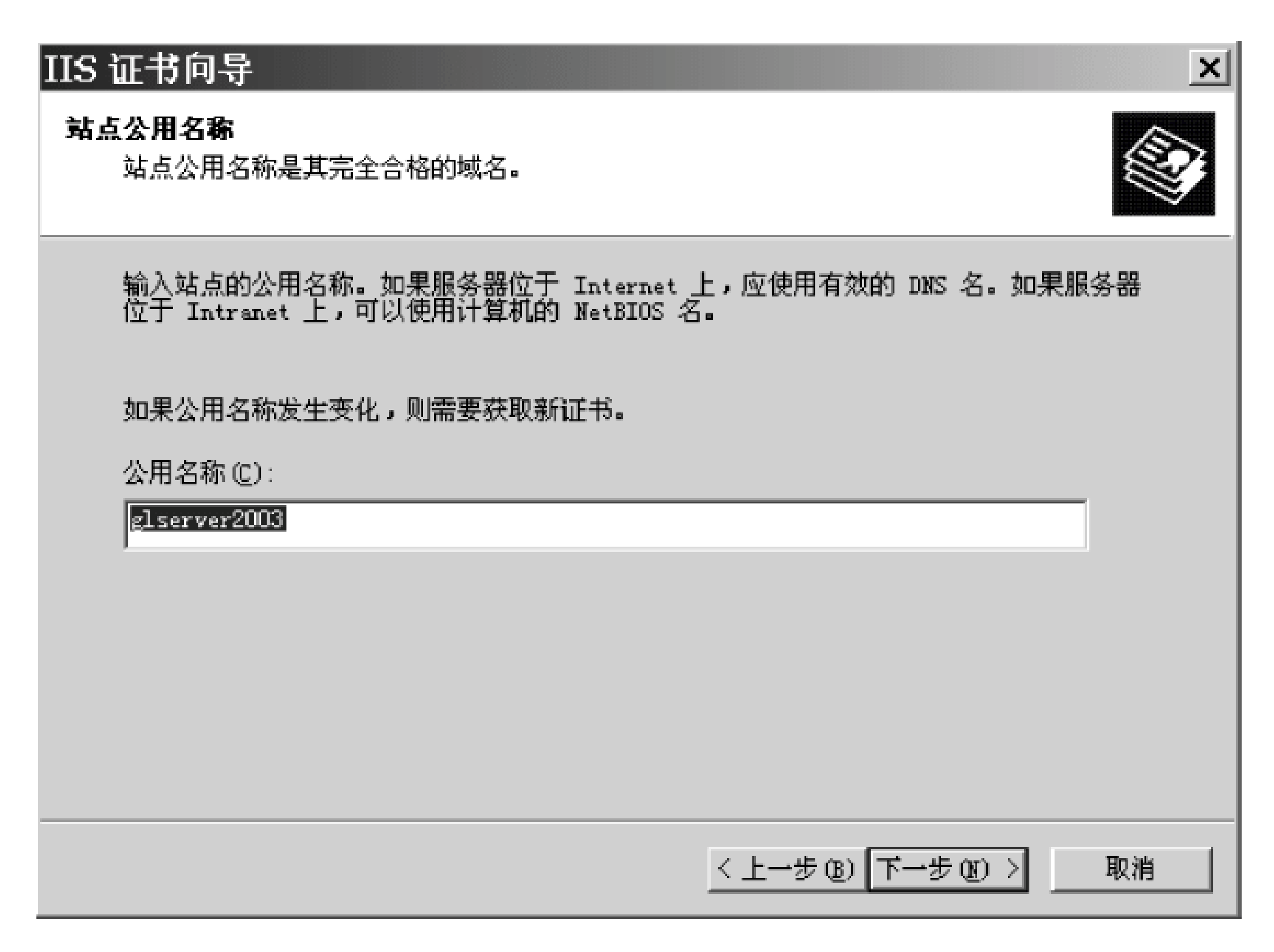


图 11-21 “站点公用名称”对话框

注意:公用名是证书最重要的信息之一。它是 Web 站点的 DNS 名称,即用户在浏览 Web 站点时键入的名称。如果证书名称与站点名称不匹配,当用户浏览到 Web 站点时,将报告证书问题。例如,如果 Web 站点的域名为 www.test.com,www.test.com 就是应当指定的公用名。若公用名称发生变化,需要获取新证书。此处因为 Web 服务器的机器名是 glserver2003,所以公用名称设为 glserver2003。

⑥ 单击“下一步”按钮,弹出“地理信息”对话框,根据实际情况填写相关信息,如图 11-22 所示。

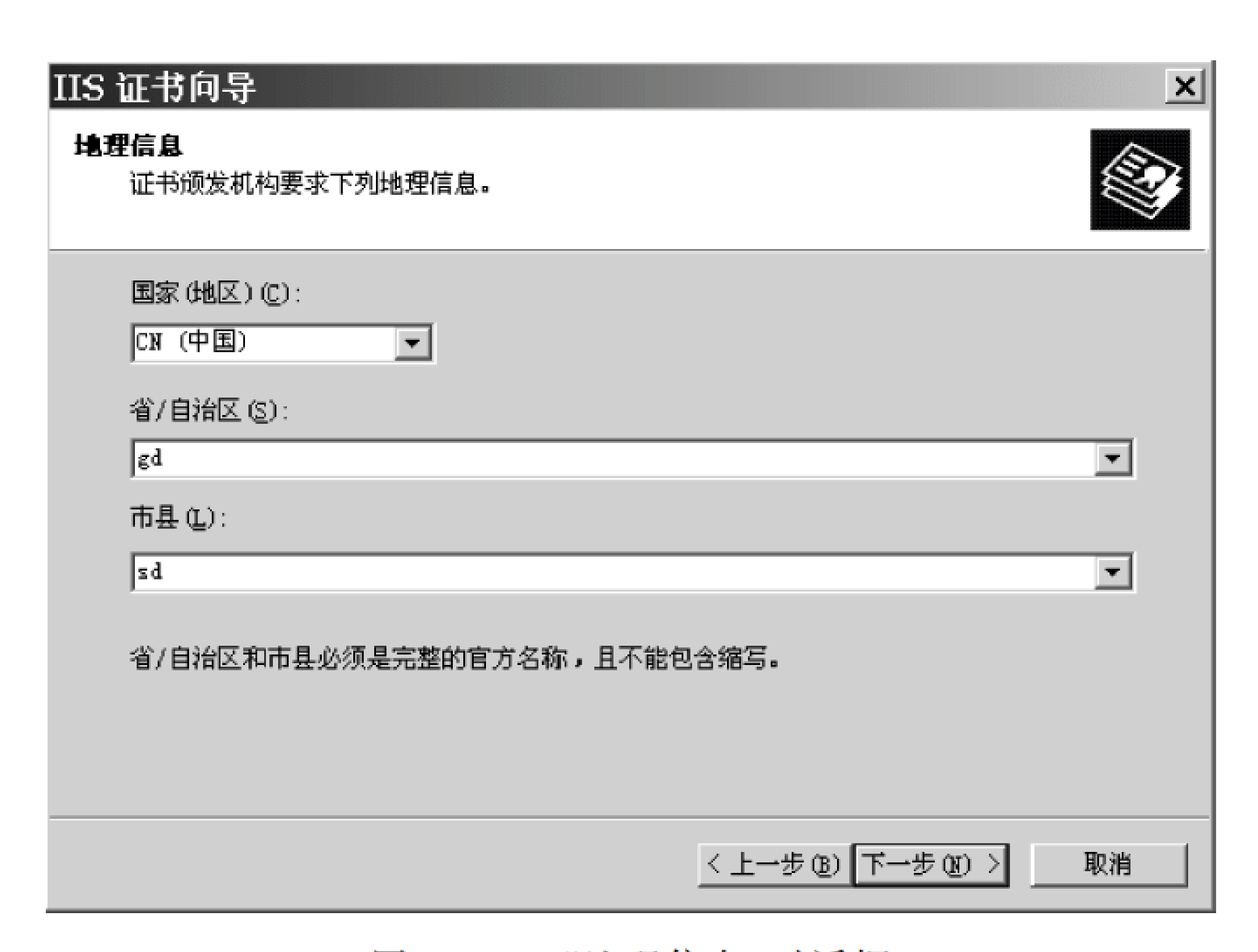


图 11-22 “地理信息”对话框

⑦ 单击“下一步”按钮,弹出“证书请求文件名”对话框,用来指定要保存的证书请求文件的文件名和路径。默认保存在 C:\certreq.txt 文件中。

⑧ 单击“下一步”按钮，显示“请求文件摘要”对话框，确认前面设置的所有信息。然后单击“下一步”按钮，完成企业 Web 服务器证书请求文件。

有了证书请求文件后，企业 Web 服务器就可以通过 IE 浏览器向证书颁发机构 CA 提交证书申请，具体操作步骤如下：

① 在企业 Web 服务器的 IE 浏览器中输入证书颁发机构 CA 的网址 http://192.168.31.111/certsrv，在弹出的“欢迎”网页中单击“申请一个证书”超链接，如图 11-23 所示。

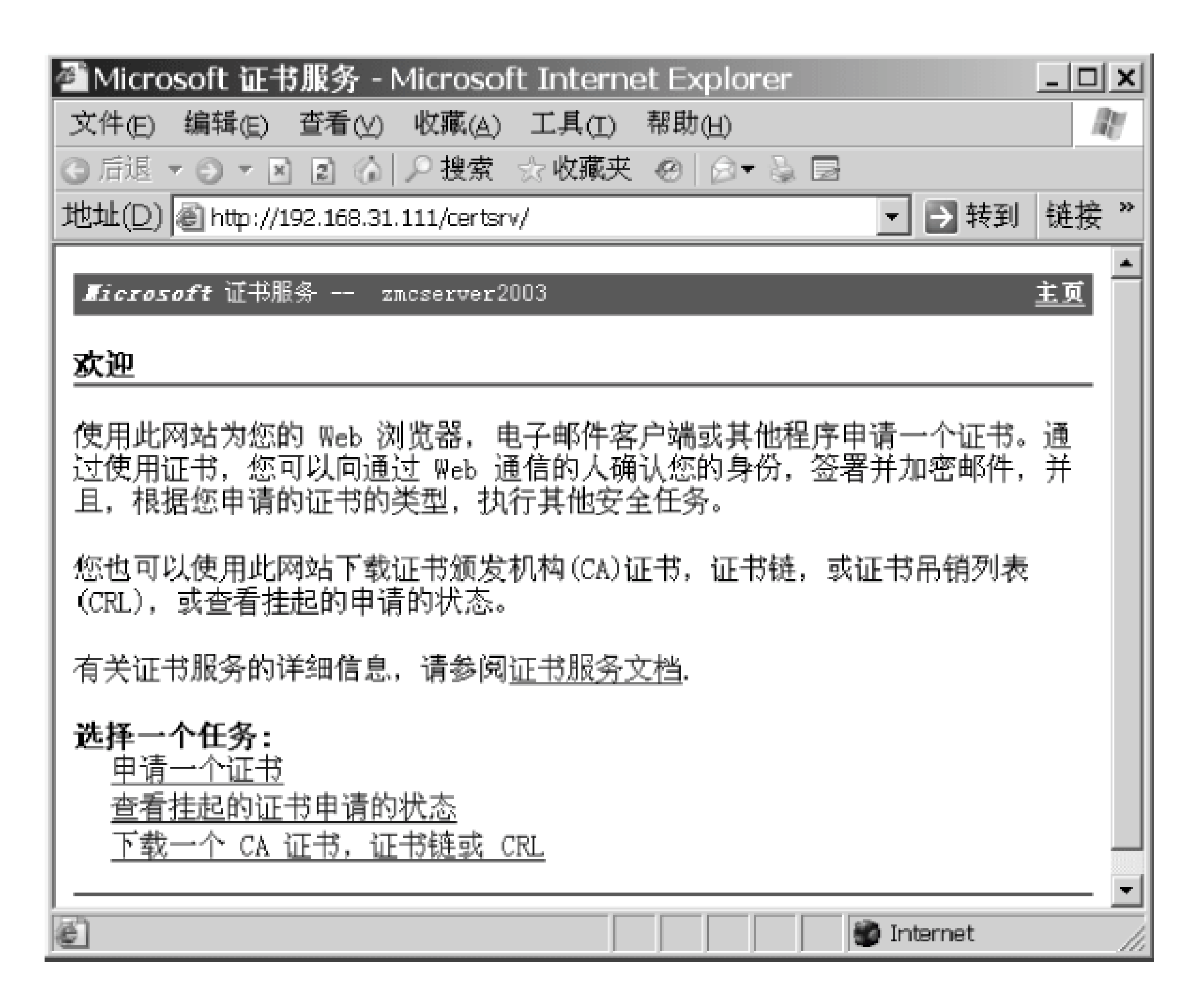


图 11-23　“欢迎”网页(1)

注意：如果打不开 CA 的网站，应检查是否能在安装证书服务的计算机上打开网站。若可以，检查两台计算机的连接情况；若不能，在控制面板重装 IIS，重装证书服务。

② 单击“下一步”按钮，弹出“申请一个证书”窗口，选择“高级证书申请”选项，如图 11-24 所示。



图 11-24　“申请一个证书”窗口

③ 单击“下一步”按钮，在弹出的窗口中选择“使用 base64 编码的 CMC 或 PKCS＃10 文件提交一个证书申请，或使用 base64 编码的 PKCS＃7 文件续订证书申请”，如图 11-25 所示。

④ 在出现的“提交一个证书申请或续订申请”界面中，将前面保存的服务器证书请求文件 C:\certreq.txt 中的内容完整复制到“保存的申请”文本框中，如图 11-26 所示。

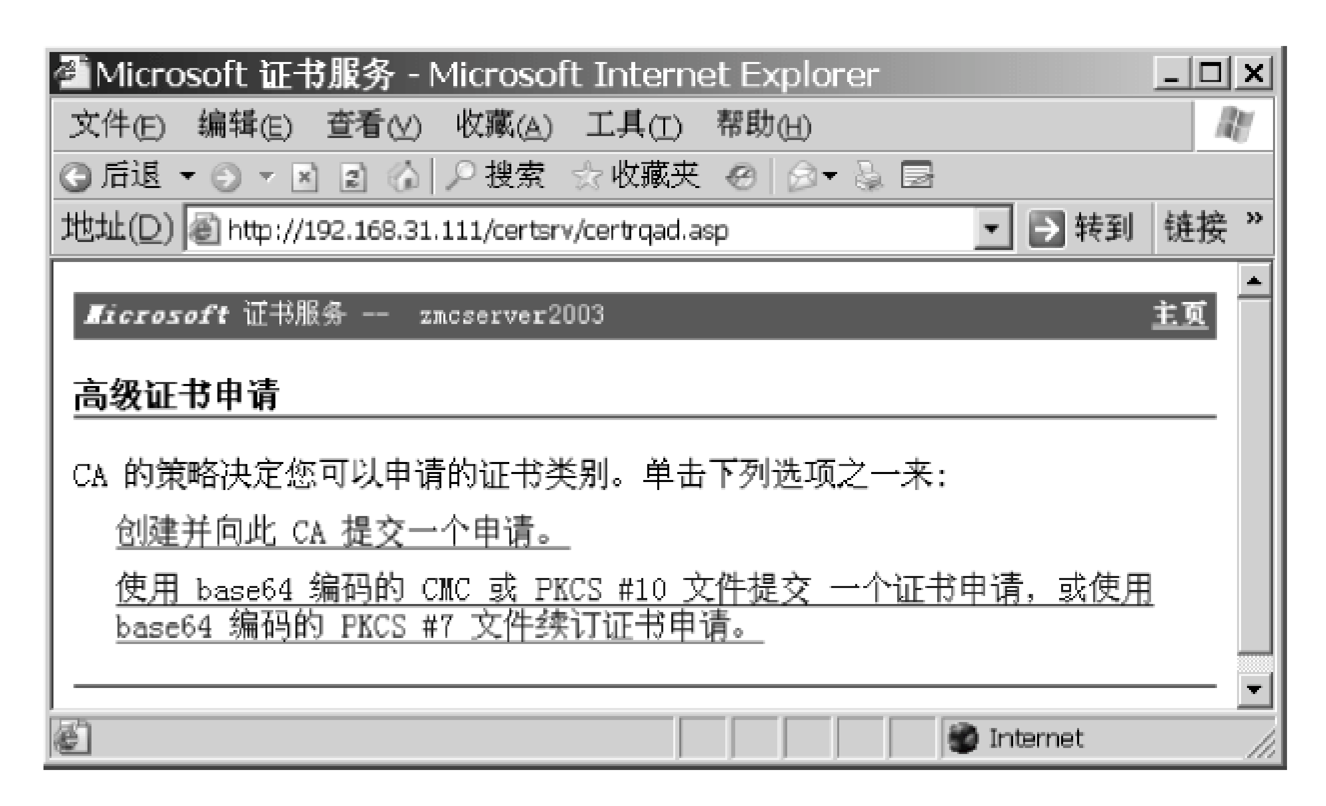


图 11-25 “高级证书申请”窗口



图 11-26 “提交一个证书申请或续订申请”窗口

⑤ 单击“提交”按钮，弹出“证书挂起”窗口界面，如图 11-27 所示。此时，证书申请已被证书颁发机构 CA 收到，需要等待管理员颁发证书。

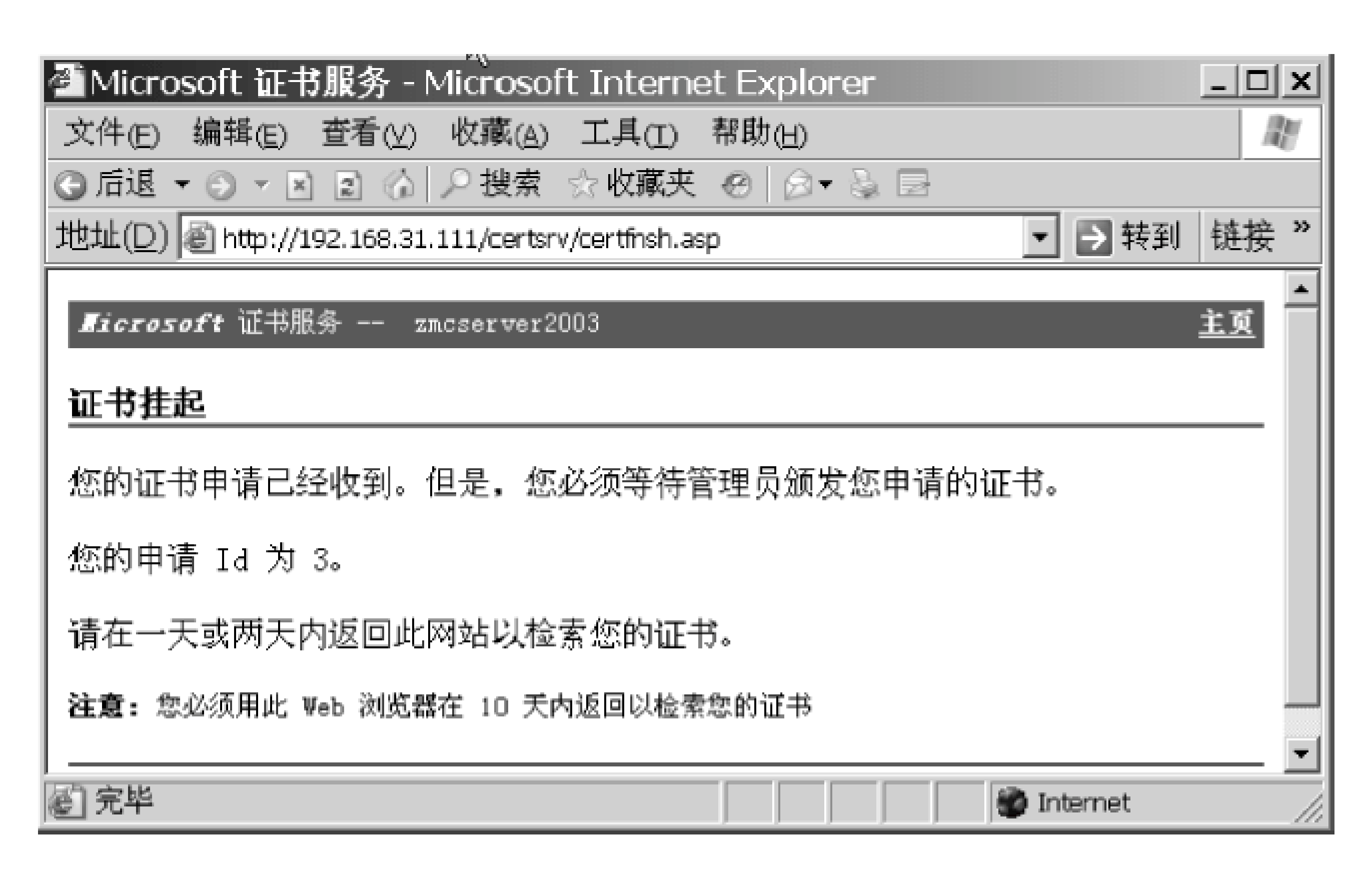


图 11-27 “证书挂起”窗口

证书颁发机构 CA 颁发证书的具体操作步骤如下：

① 在证书颁发机构 CA 的计算机中单击“开始”→“所有程序”→“管理工具”命令，打开“证书颁发机构”对话框，在“挂起的申请”文件夹中将看到刚才提交的 Web 服务器证书申请。

② 在该证书上右击，在弹出的快捷菜单中选择“所有任务”→“颁发”命令，颁发此证书，如图 11-28 所示。

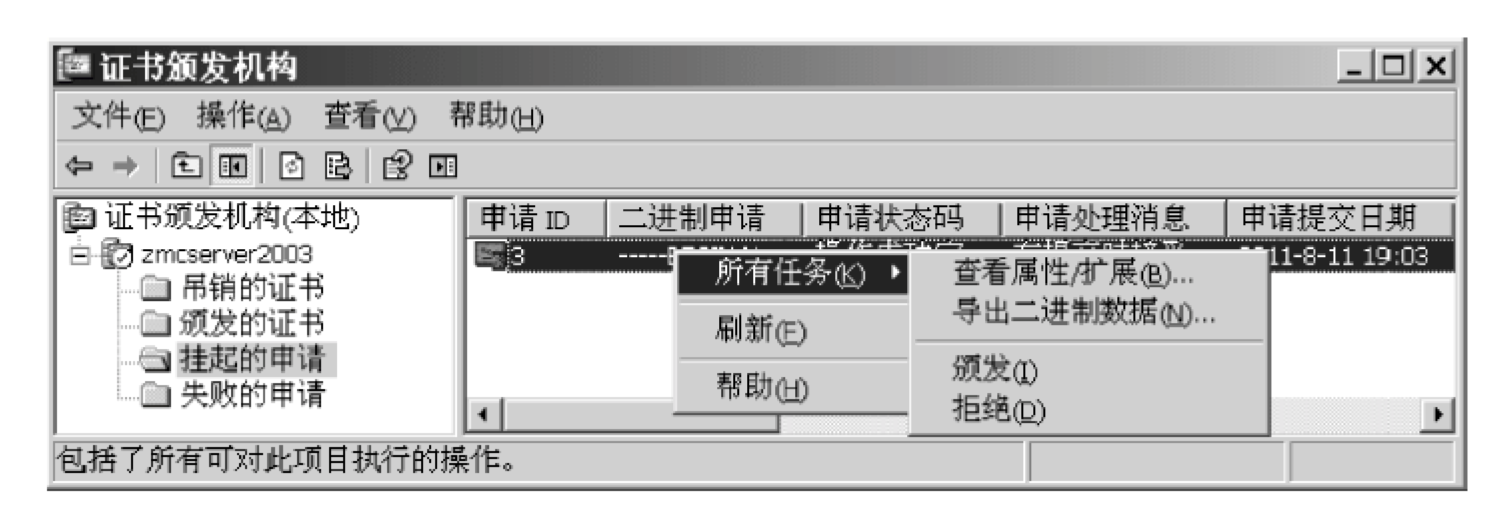


图 11-28　“挂起的申请”窗口

③ 管理员颁发证书后，在“颁发的证书”窗口中就能看到已经颁发了的证书，如图 11-29 所示。

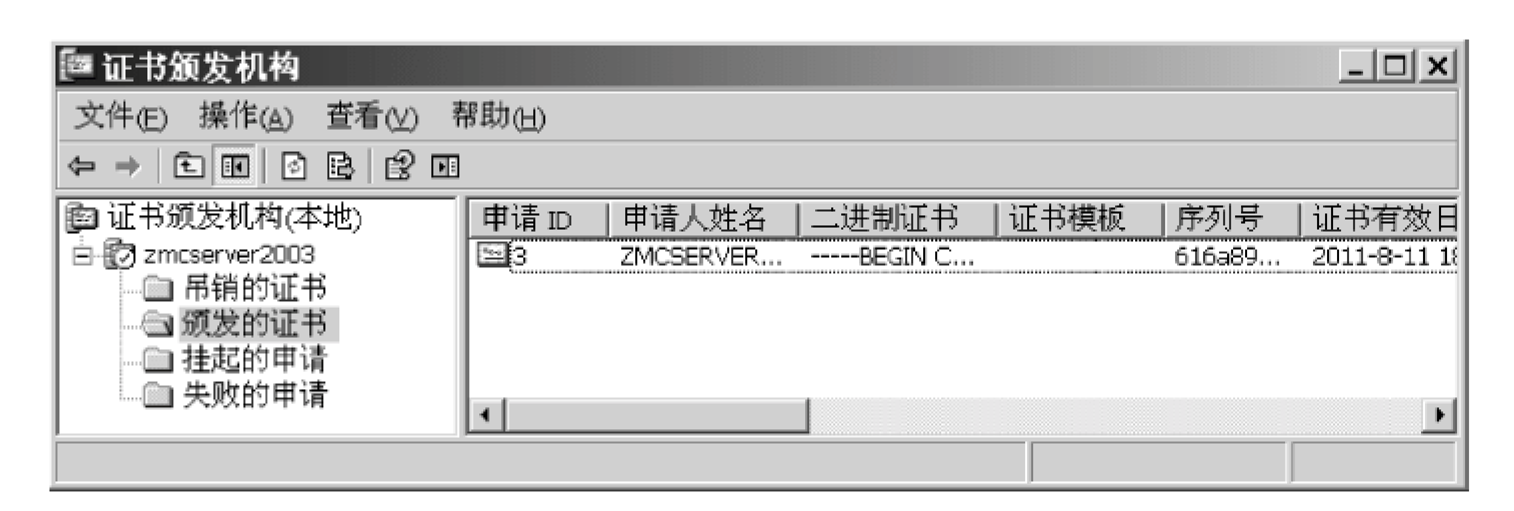


图 11-29　“颁发的证书”窗口

然后，在企业 Web 站点可以下载并安装该证书，具体的操作步骤如下：

① 在企业 Web 服务器的 IE 浏览器中输入证书颁发机构 CA 的网址 http://192.168.31.111/certsrv，在弹出的“欢迎”网页中单击“查看挂起的证书申请的状态”超链接，如图 11-30 所示。

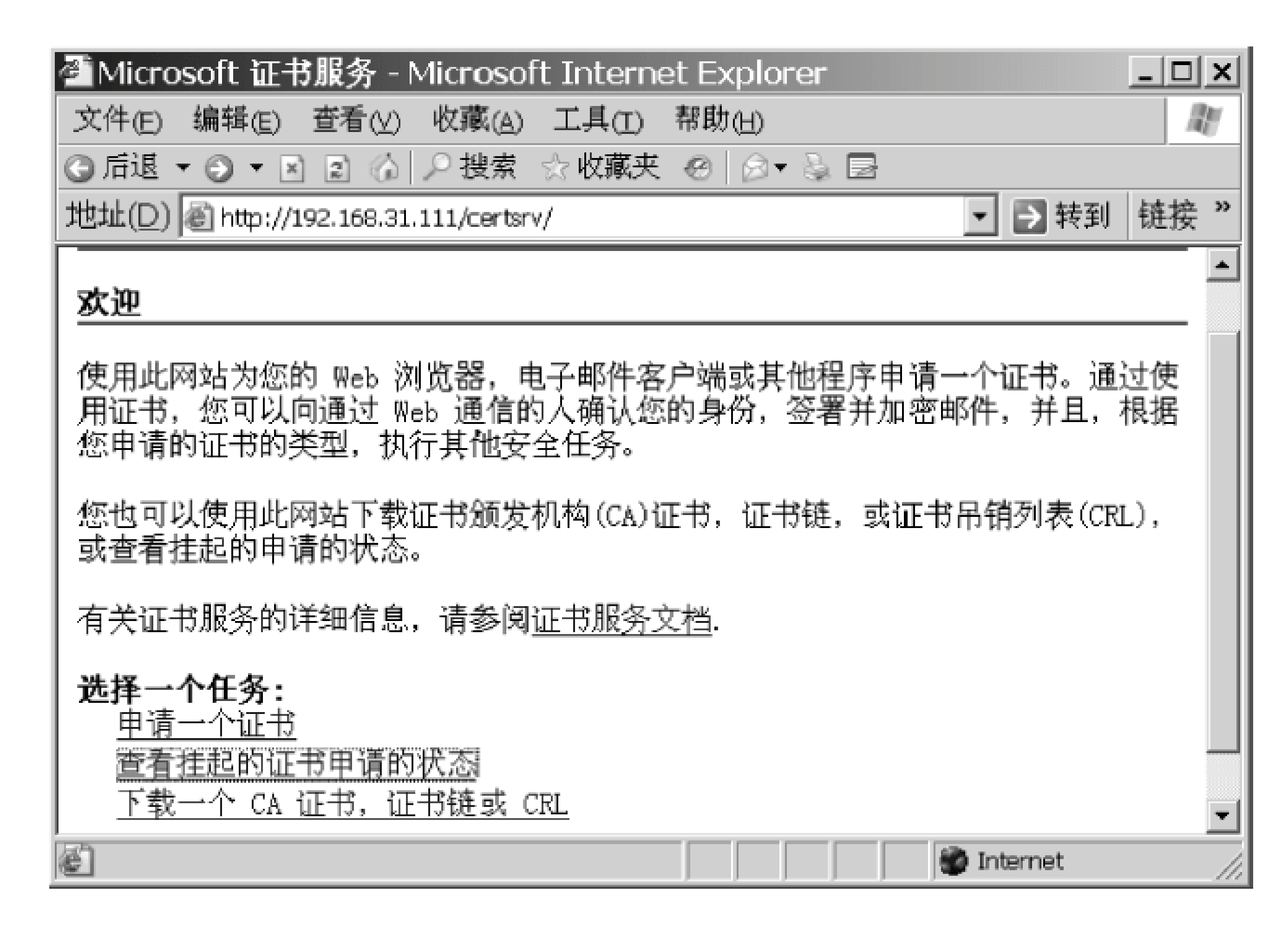


图 11-30　“欢迎”网页(2)

② 在弹出的“查看挂起的证书申请的状态”网页中根据申请的时间选择“保存的申请证书”超链接，如图 11-31 所示。



图 11-31 “查看挂起的证书申请的状态”网页

③ 在弹出的“证书已颁发”网页中选择“下载证书”，如图 11-32 所示。



图 11-32 “证书已颁发”网页

④ 弹出“文件下载”窗口，单击“保存”按钮，如 11-33 所示。

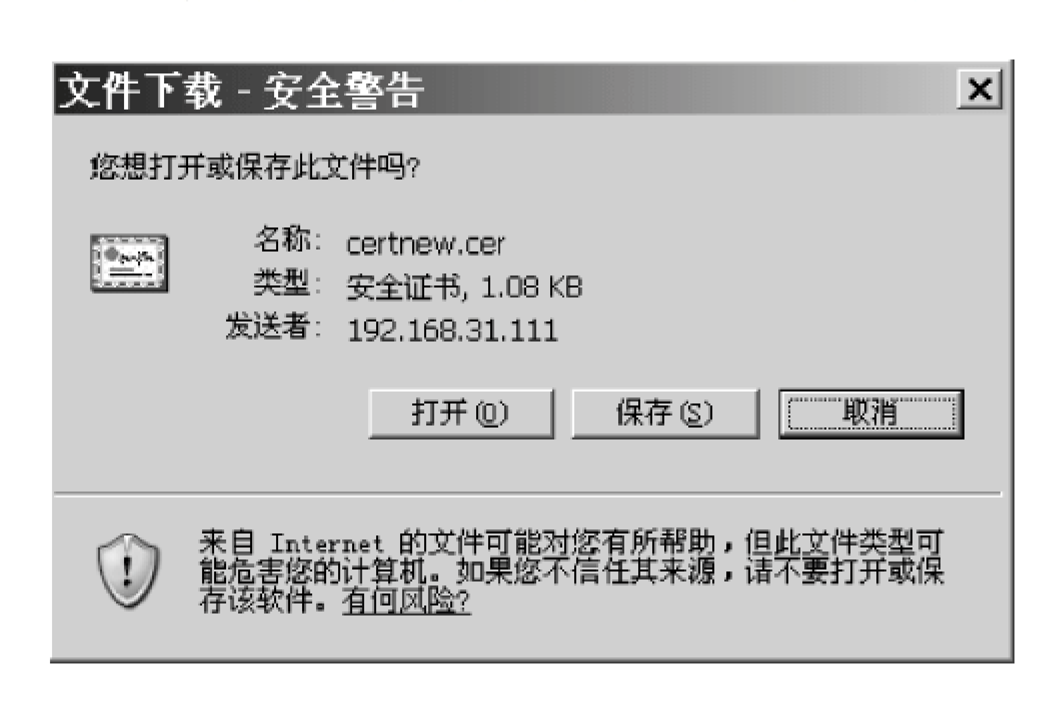


图 11-33 “文件下载”窗口

⑤ 选择保存证书的路径和名称，然后单击“确定”按钮。

⑥ 打开企业 Web 站点的 Internet 信息服务(IIS)管理器，在 Web 站点的“目录安全性”选项卡中单击“安全通信”选项区域的“服务证书”按钮，启动 Web 服务器证书向导，通过该向导来安装刚刚导出的服务器证书。

⑦ 在“挂起的证书请求”对话框中，选中“处理挂起的请求并安装证书”选项，如图 11-34 所示。

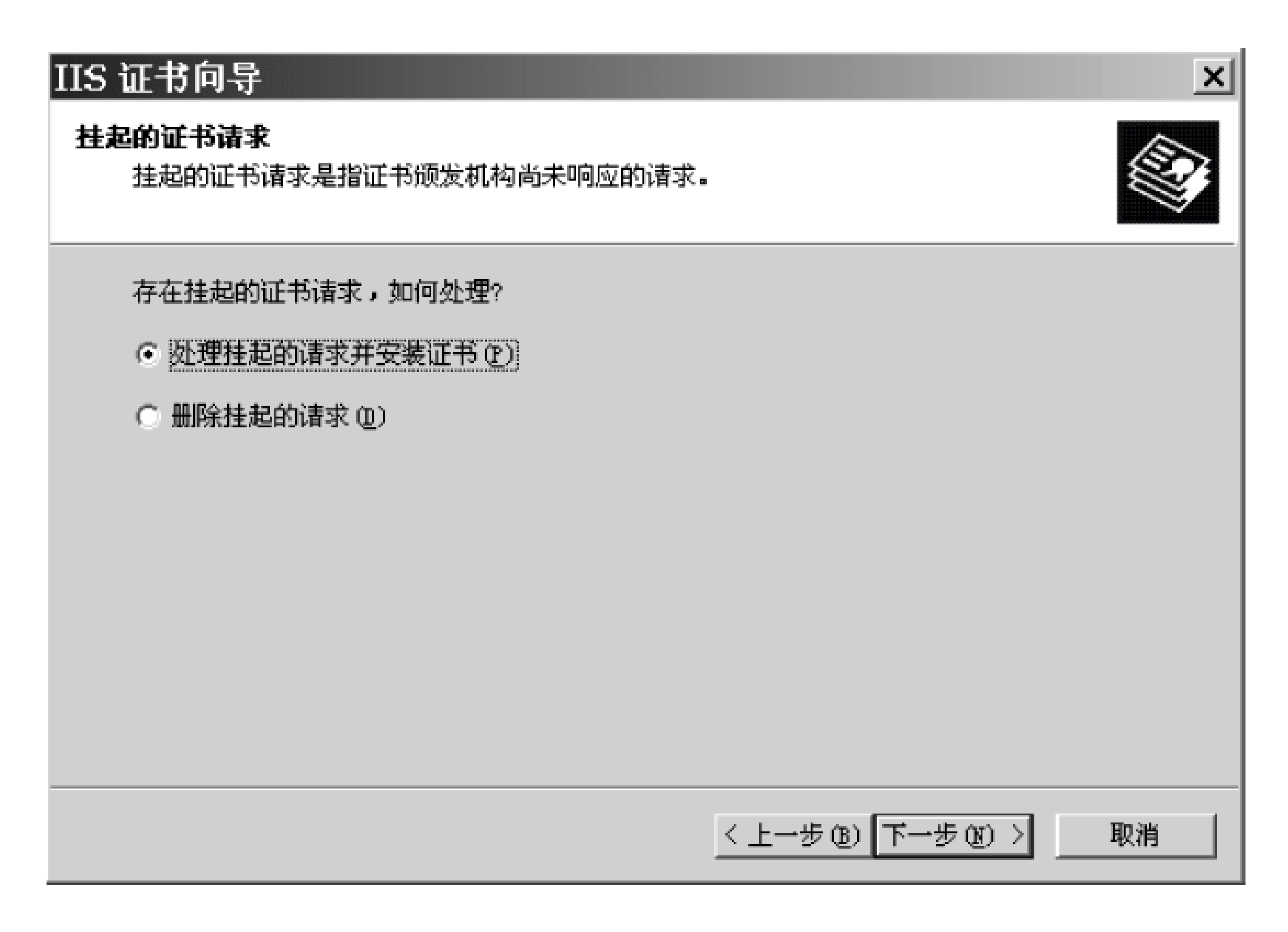


图 11-34　“挂起的证书请求”对话框

⑧ 单击“下一步”按钮，在弹出的“处理挂起的请求”对话框中指定刚刚下载证书文件的路径和名称，如图 11-35 所示。

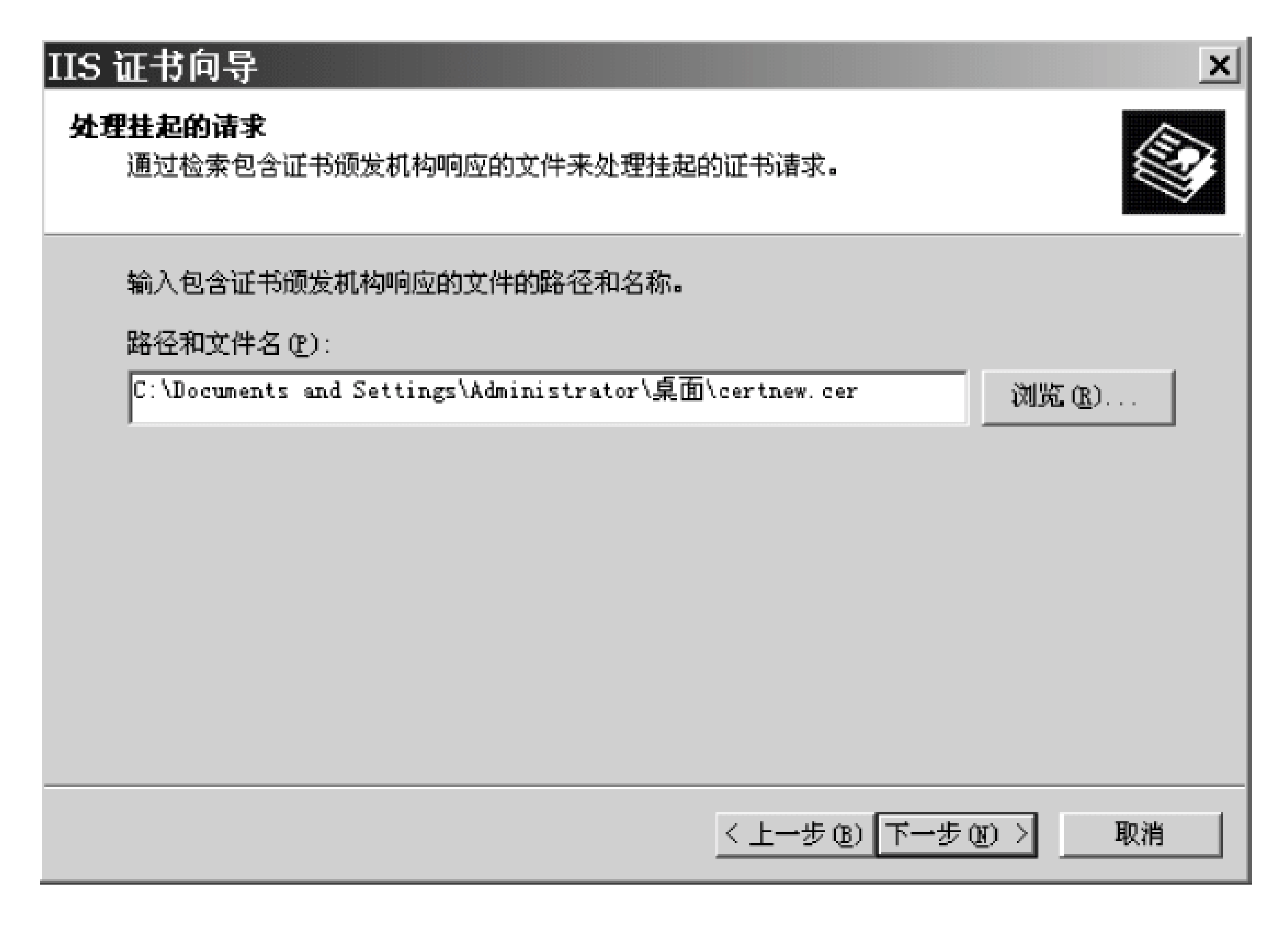


图 11-35　“处理挂起的请求”对话框

⑨ 单击“下一步”按钮，然后为 Web 站点指定 SSL 端口号为 443，如图 11-36 所示。

⑩ 单击“下一步”按钮，出现“证书摘要”窗口，如图 11-37 所示。

⑪ 单击“下一步”按钮，弹出“完成 Web 服务器证书向导”对话框。单击“完成”按钮，完成 Web 服务器证书的安装。

最后，客户端将通过 SSL 安全通道建立和 Web 服务器的连接，具体操作步骤如下：

① 打开 Web 服务器的 Internet 信息服务(IIS)管理器，在 Web 站点的“目录安全性”选项卡中，单击“安全通信”选项区域的“编辑”按钮，如图 11-38 所示。

② 打开“安全通信”对话框，在该对话框中选中“要求安全通道(SSL)”和“要求 128 位加密”，并单击“确定”按钮，如图 11-39 所示。

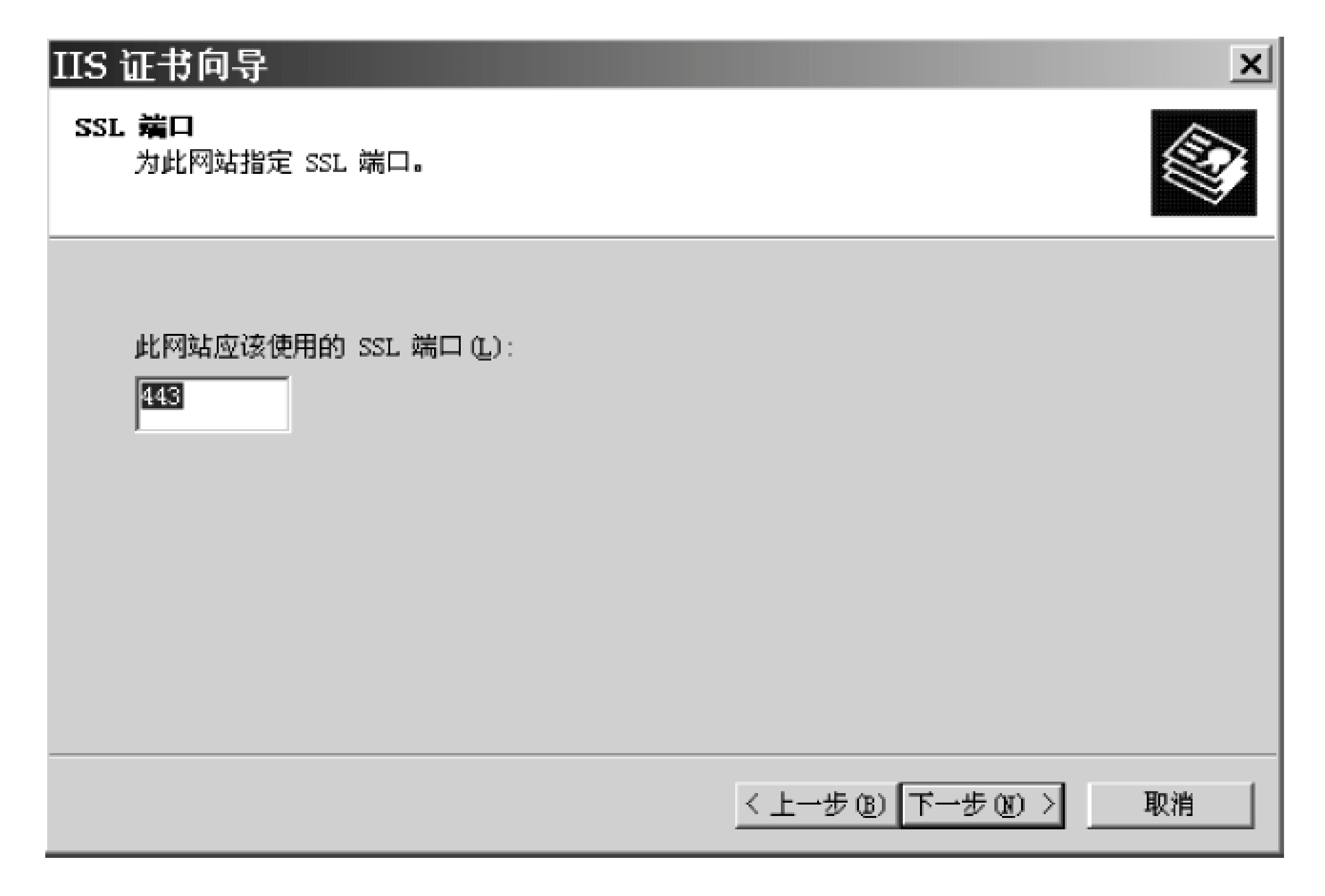


图 11-36 SSL 端口设置

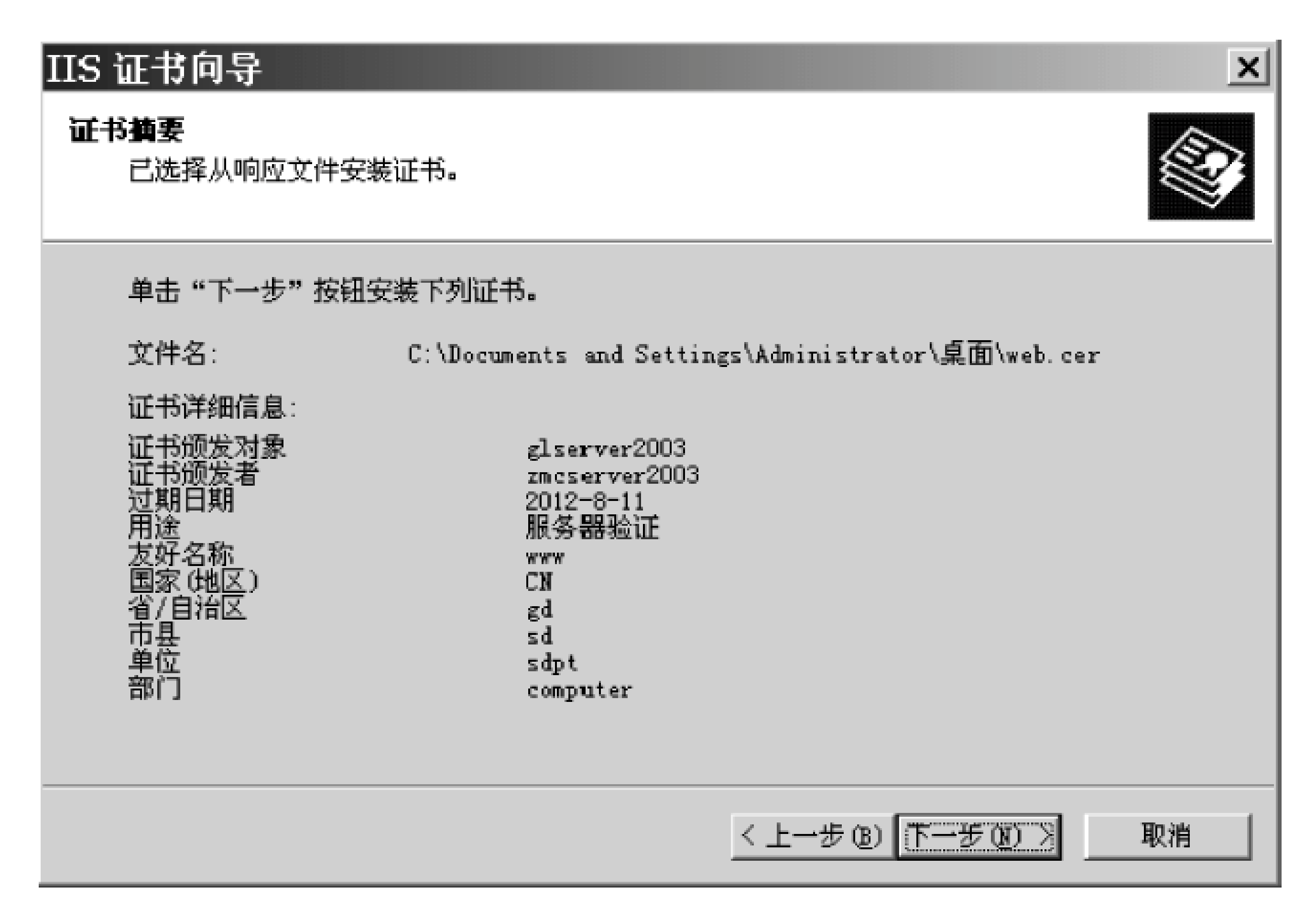


图 11-37 “证书摘要”窗口

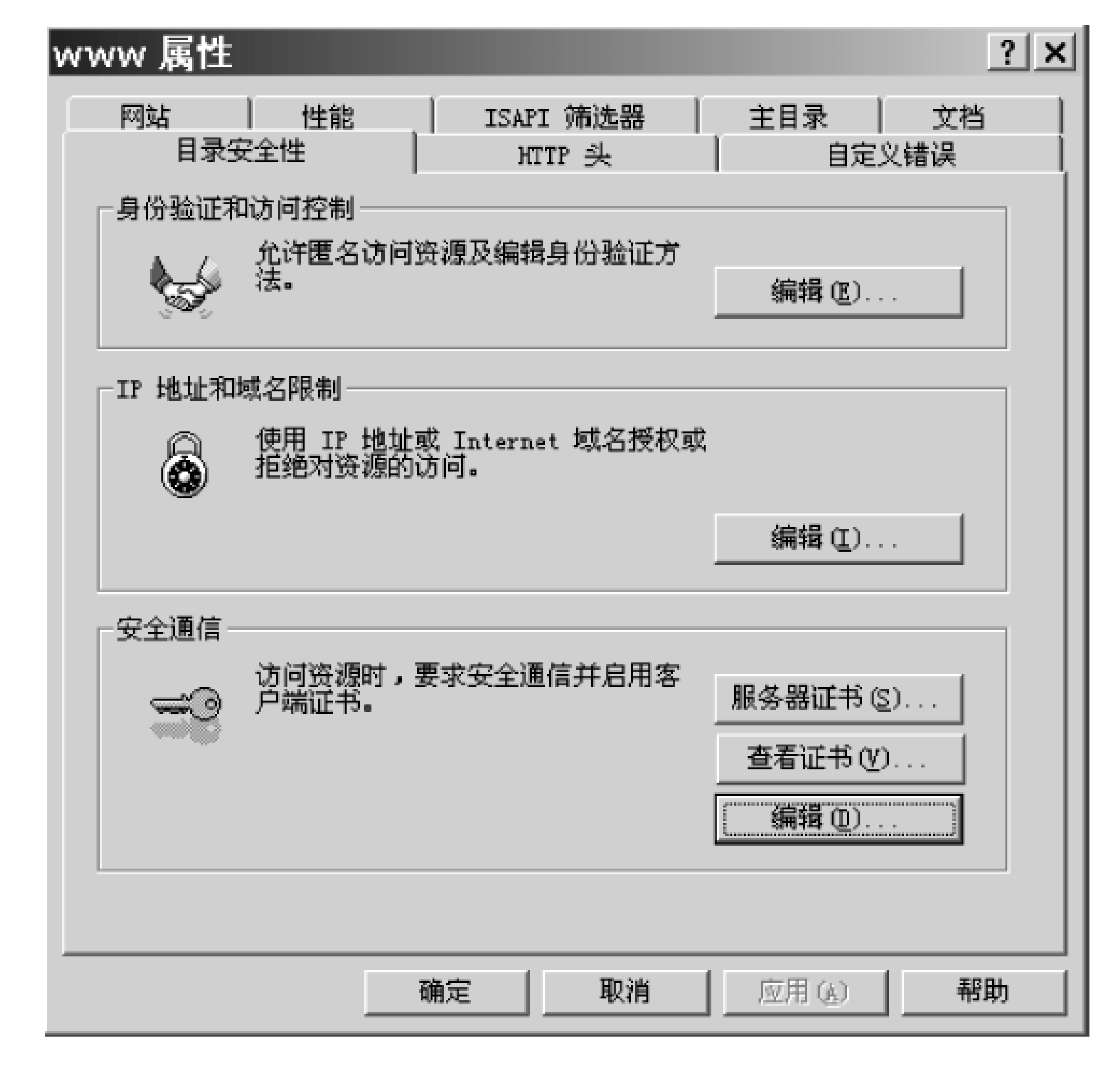


图 11-38 “目录安全性”选项卡



图 11-39 “安全通信”对话框

③ 在客户机的 IE 浏览器中输入“http://192.168.31.3”来访问企业 Web 站点，将显示“该页必须通过安全通道查看”，如图 11-40 所示。

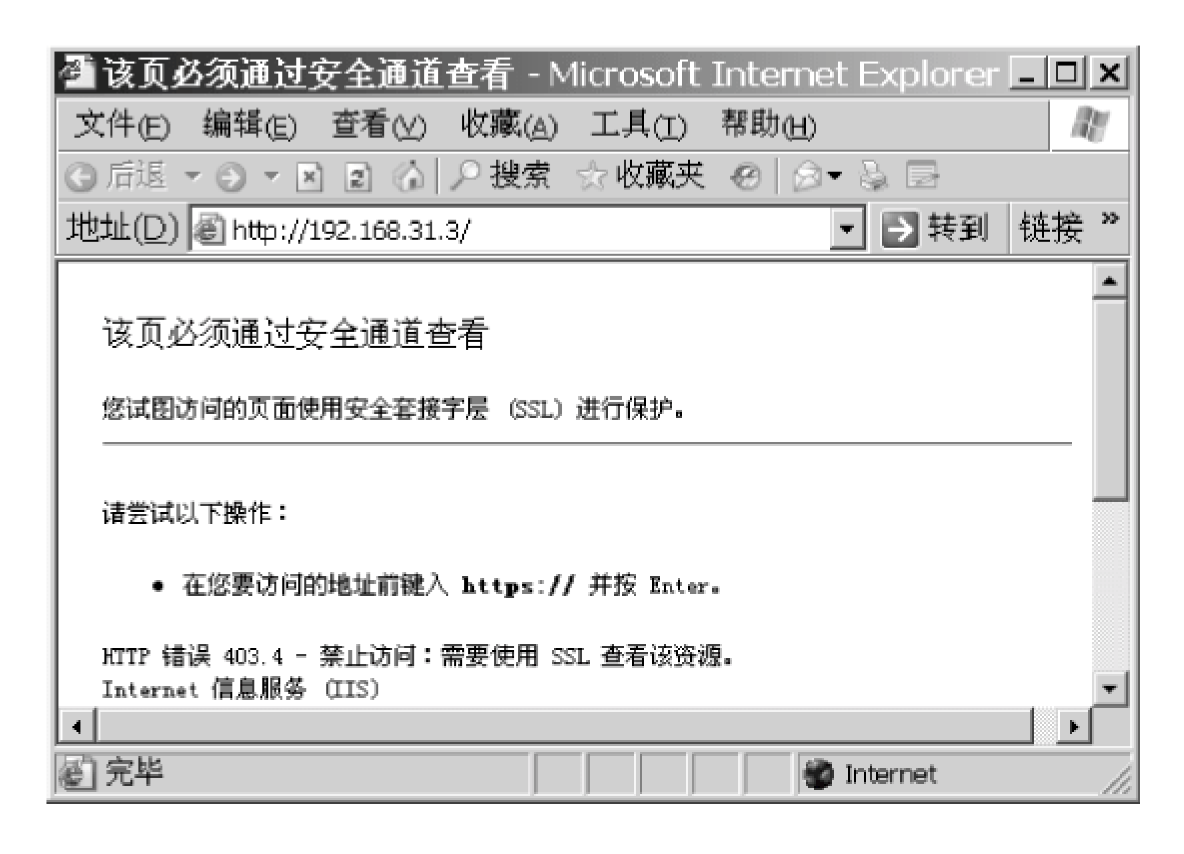


图 11-40　安全提示(1)

④ 客户机必须通过 SSL 安全通道建立和 Web 站点的通信。在客户机的 IE 浏览器中输入“https://192.168.31.3”来访问企业 Web 站点，出现如图 11-41 所示安全警报。

⑤ 如果单击“是”按钮，表示客户机信任了证书持有人 Web 站点证书的合法性。单击“查看证书”按钮，打开“证书信息”对话框以查看证书的相关信息，从而决定是否通过验证，如图 11-42 所示。

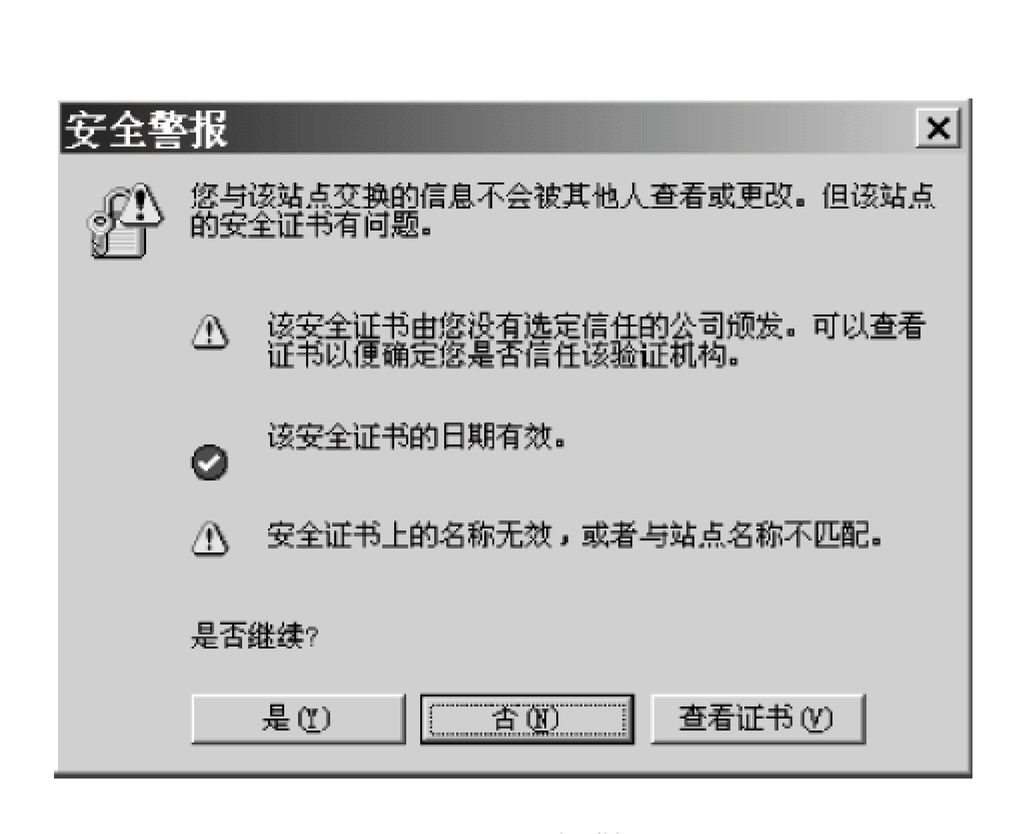


图 11-41　安全警报(1)

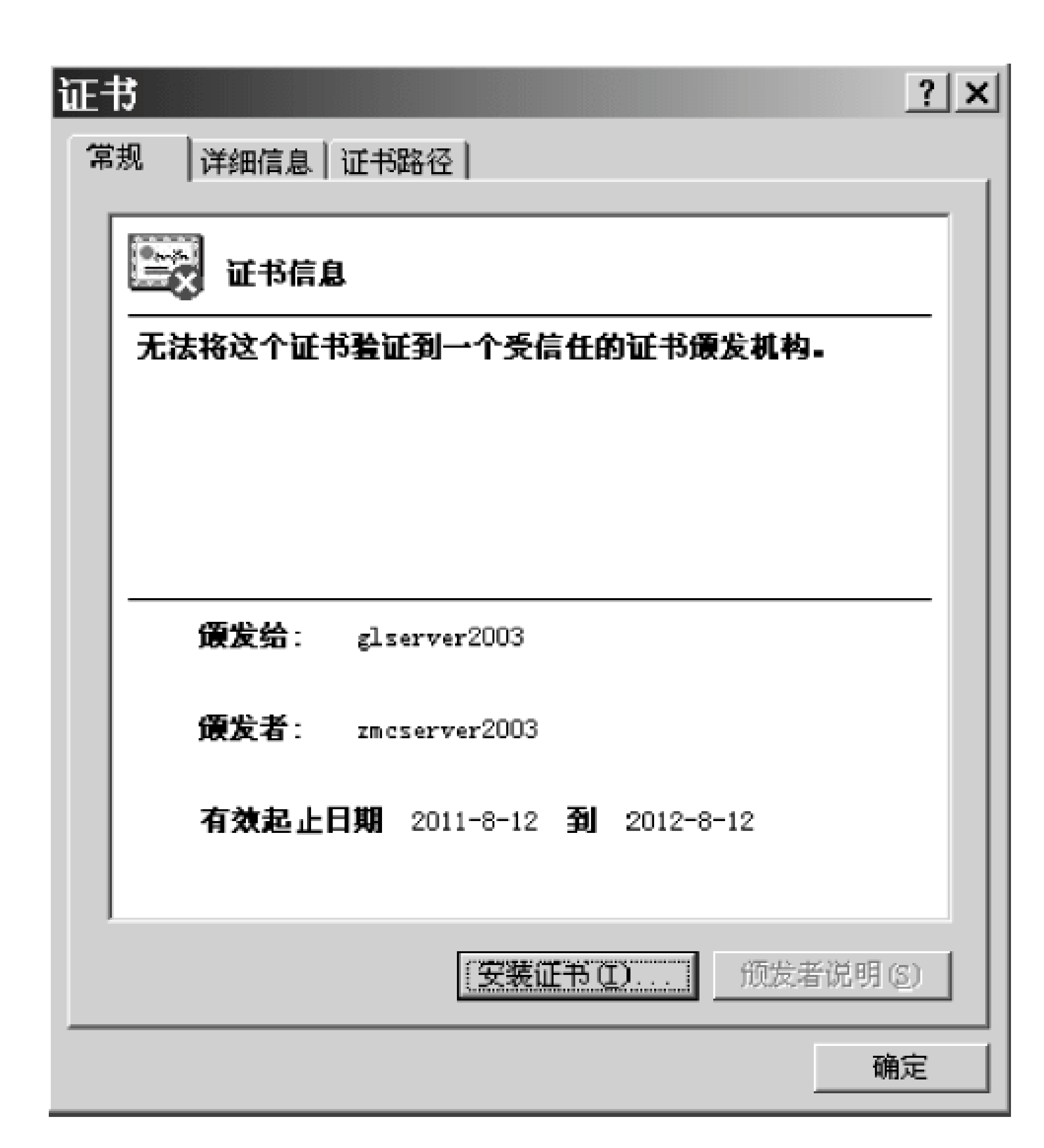


图 11-42　证书信息(1)

从图 11-41 可以看到有两个感叹号表示的警告标识，第一个是由于该证书不是由客户机所信任的根证书颁发机构所颁发，第二个是由于在客户机的 IE 浏览器中输入的访问站点名称和证书所有者的名称不一致。

消除第一个警告标识，需要将根证书颁发机构的证书导出，并安装到客户机证书存储区的“受信任的根证书颁发机构”中，具体的操作步骤如下：

① 在“证书颁发机构”对话框中，右击证书颁发机构，然后选择“属性”选项，如图11-43所示。

② 在“属性”界面中，选择“常规”选项卡，并单击“查看证书”按钮，可以看到证书的详细信息，如图11-44所示。

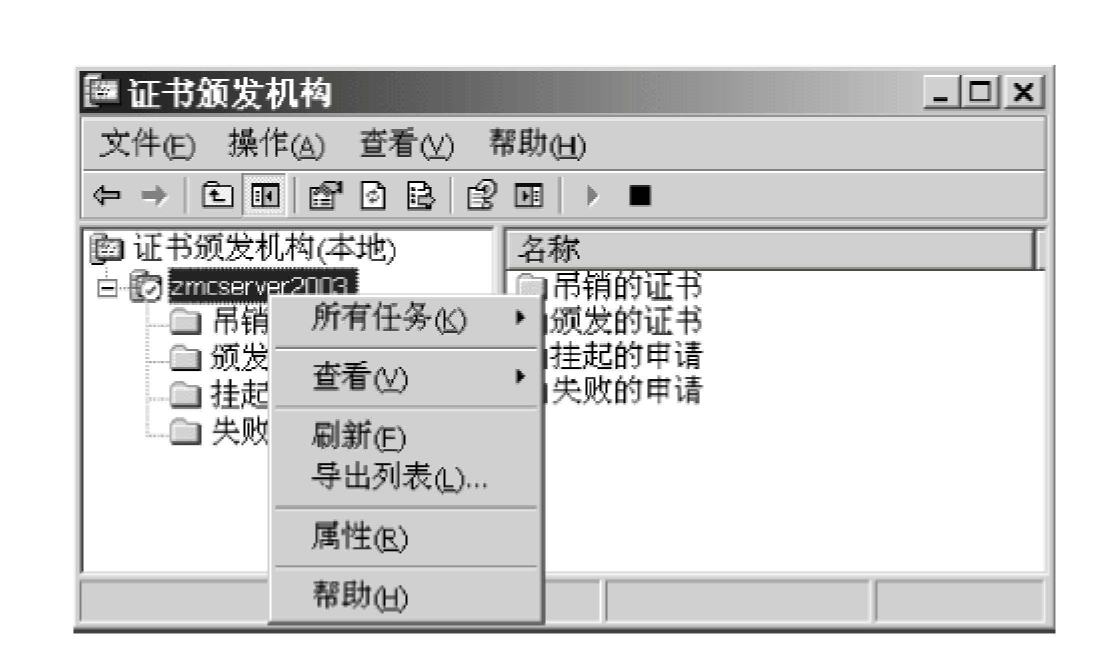


图 11-43 “证书颁发机构”对话框



图 11-44 证书信息(2)

③ 选择“详细信息”选项卡并单击“复制到文件”按钮，启动证书导出向导。选择“加密消息语法标准-PKCS＃7证书”的文件格式，如图11-45所示。

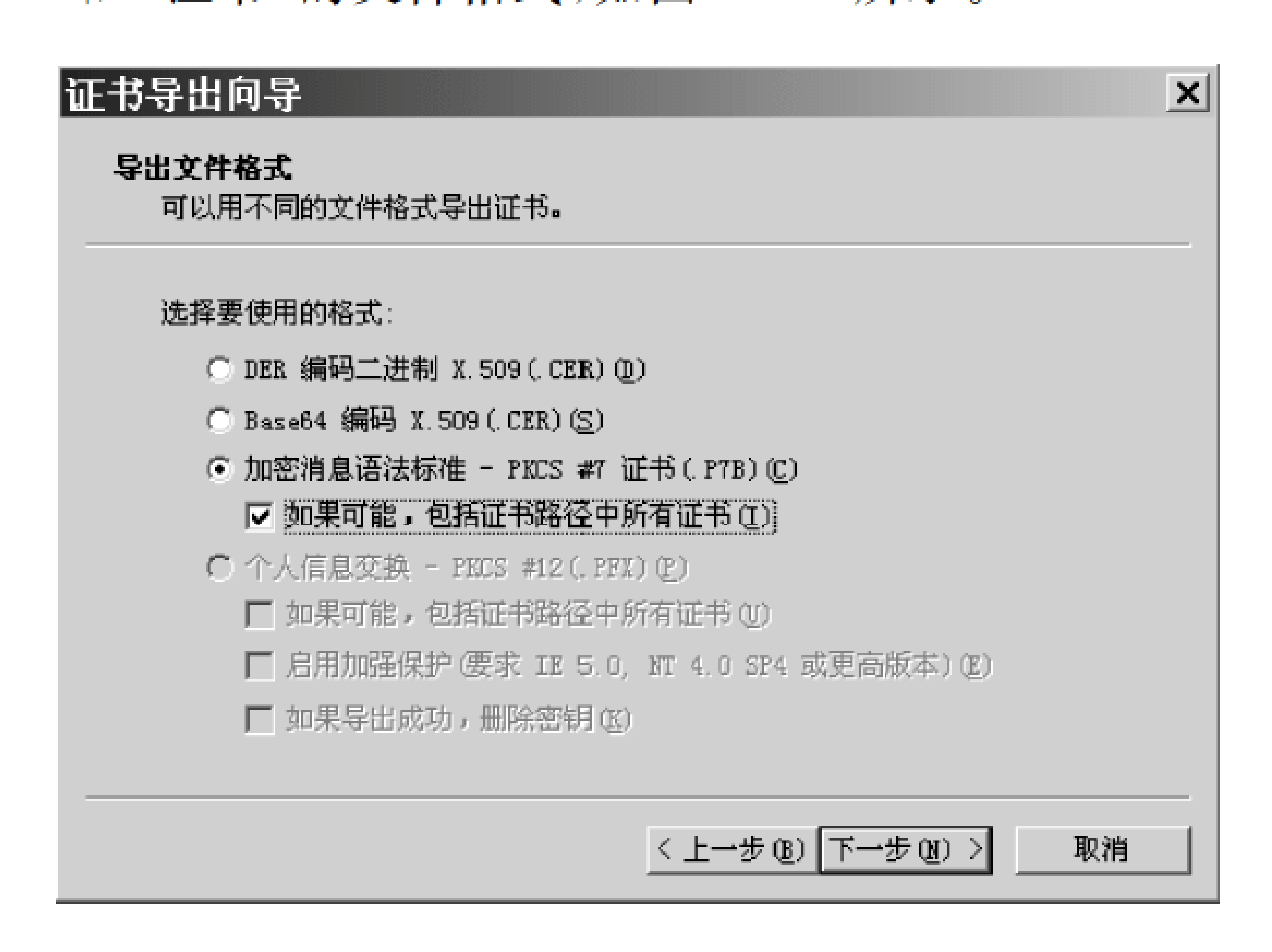


图 11-45 “证书导出向导”对话框

④ 单击“下一步”按钮，将该证书导出为C:\root.p7b文件，如图11-46所示，并发送给客户机。

⑤ 在客户机上打开IE浏览器，然后选择“工具”→“Internet选项”菜单项，在弹出的对话框中选择“内容”选项卡，如图11-47所示。

⑥ 单击“证书”按钮，打开证书信息对话框，然后选择“受信任的根证书颁发机构”选项卡，如图11-48所示。

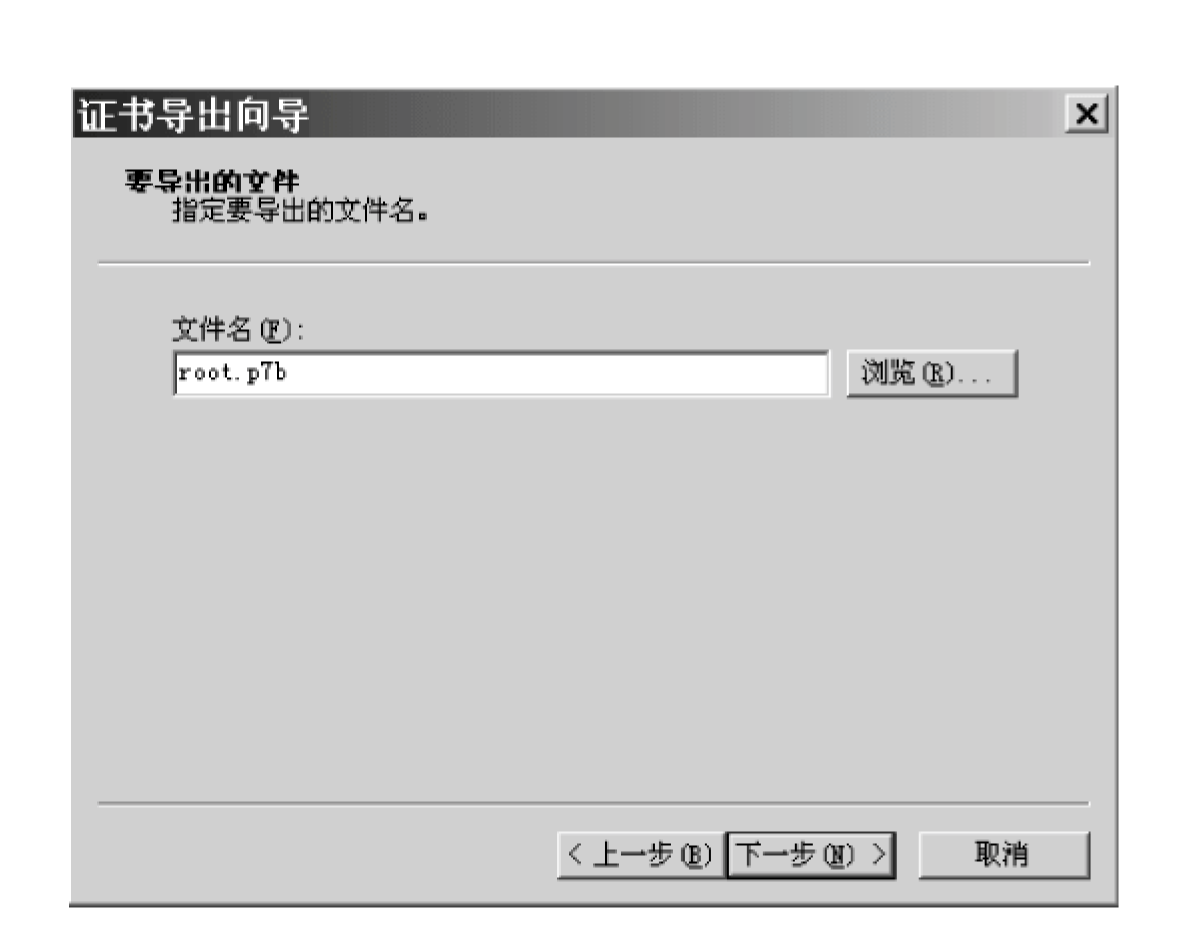


图 11-46 指定要导出的文件名



图 11-47 “内容”选项卡



图 11-48 “受信任的根证书颁发机构”选项卡

⑦ 单击“导入”按钮，将从证书颁发机构导出的 CA 证书文件 C:\root.p7b 导入到客户机的证书存储区，如图 11-49 所示，此时表示客户机已经信任了该 CA 颁发的证书。

⑧ 再通过“https://192.168.31.3”来访问企业 Web 站点，就不会出现第一个安全警告标识，如图 11-50 所示。

消除第二个警告标识的方法很简单，只需在访问企业 Web 站点时输入站点的 DNS 名或计算机 NetBIOS 名称即可。如果服务器位于互联网，则输入 DNS 名；如果服务器位于 Intranet，则输入计算机的 NetBIOS 名，使输入的站点名称和安全证书上的所有者名称保持一致，即输入“https://glserver2003”就不会出现安全警告了。

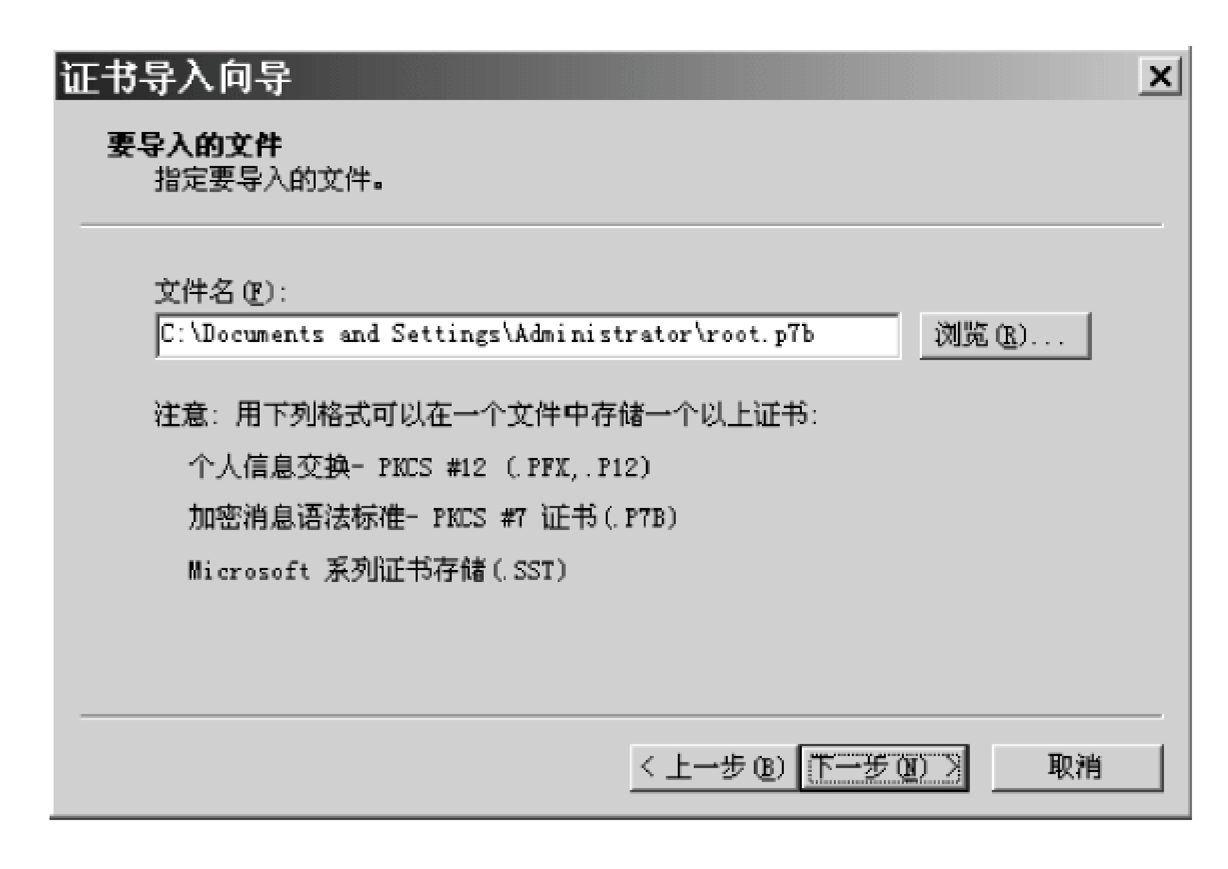


图 11-49　指定要导入的文件

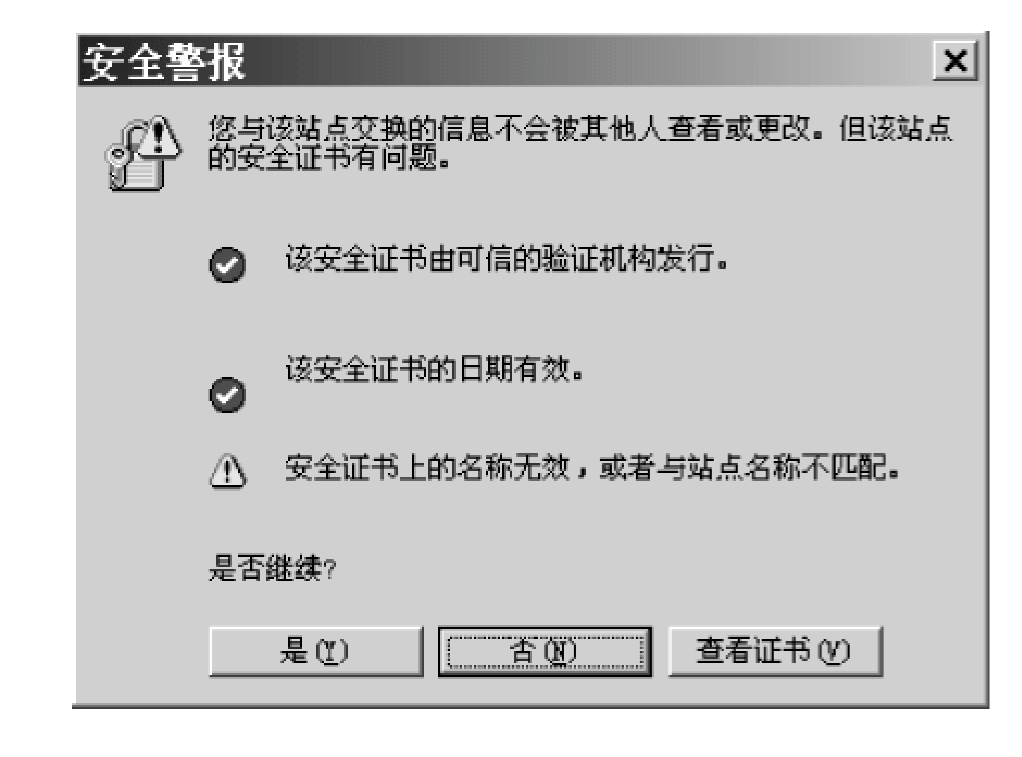


图 11-50　安全警报(2)

前面介绍了企业 Web 站点向客户端用户证明身份的服务器证书的安装。下面介绍客户端向 Web 站点服务器证明自己身份的客户端证书的安装，具体操作步骤如下：

① 在企业 Web 服务器端的计算机上，打开 Internet 信息服务(IIS)管理器，然后在 Web 站点的“目录安全性”选项卡中单击“安全通信”选项区域的“编辑”按钮，打开“安全通信”对话框。在对话框内选中“要求客户端证书”，如图 11-51 所示。

② 客户端计算机打开 IE 浏览器，输入“https://192.168.31.3”访问 Web 站点，会弹出“选择数字证书”对话框，如图 11-52 所示。



图 11-51　“安全通信”对话框



图 11-52　“选择数字证书”对话框

如果没有安装客户端证书，则没有可以选择的证书，直接单击“确定”按钮，会弹出“该页需要客户证书”提示，无法访问。

为了在客户机上申请安装客户证书，先在 Web 服务器上撤选“要求服务端证书”，改选“忽略客户端证书”。

③ 在客户机上访问“https://192.168.31.3/certsrv”，然后单击“申请一个证书”超级链接，并选择申请证书类型为“Web 浏览器证书”，需要填写识别信息，最后单击“提交”按钮，如图 11-53 所示。

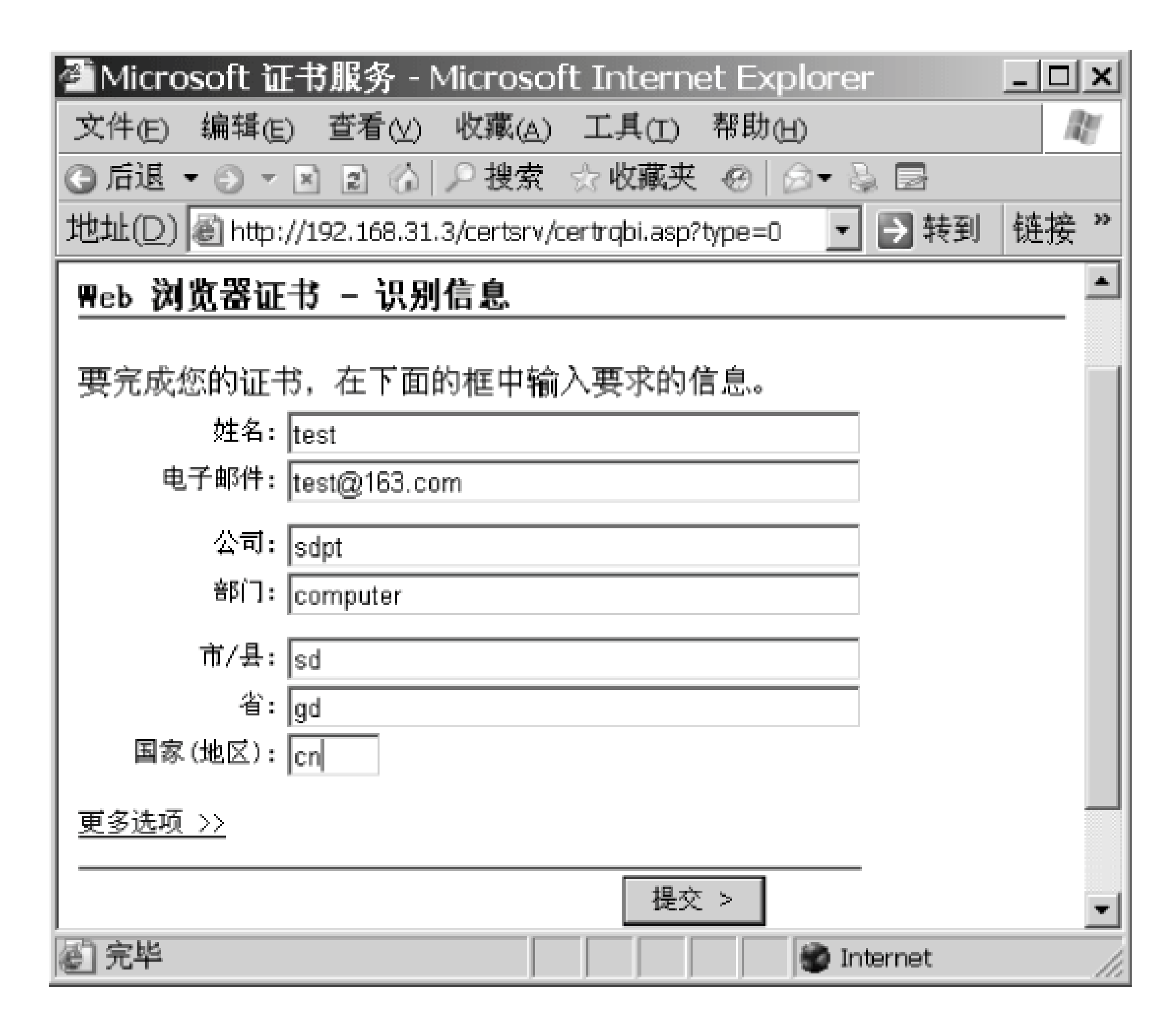


图 11-53　识别信息

④ 弹出“必须启用脚本”提示窗口，如图 11-54 所示。



图 11-54　“必须启用脚本”提示窗口

⑤ 选择 IE 浏览器右键属性，在“安全”选项卡中单击“自定义级别”按钮，在“安全设置”对话框中将脚本设置为“启用”，如图 11-55 所示。

⑥ 单击“确定”按钮，当出现证书挂起界面时，说明证书申请已被证书颁发机构 CA 收到，等待管理员颁发证书。

在证书颁发机构计算机中，审核并完成该客户端证书的颁发。CA 颁发证书后，在客户机上访问“https://192.168.31.3/certsrv”，然后单击“查看挂起的证书申请的状态”超链接，并选择刚才申请的 Web 浏览器证书。

⑦ 单击“安装此证书”超链接，完成客户端数字证书的安装。若出现“潜在的脚本冲突”提示对话框，直接单击“是”按钮。

⑧ 回到企业 Web 站点的“安全通信”对话框，选择“要求客户端证书”设置。在客户端通过

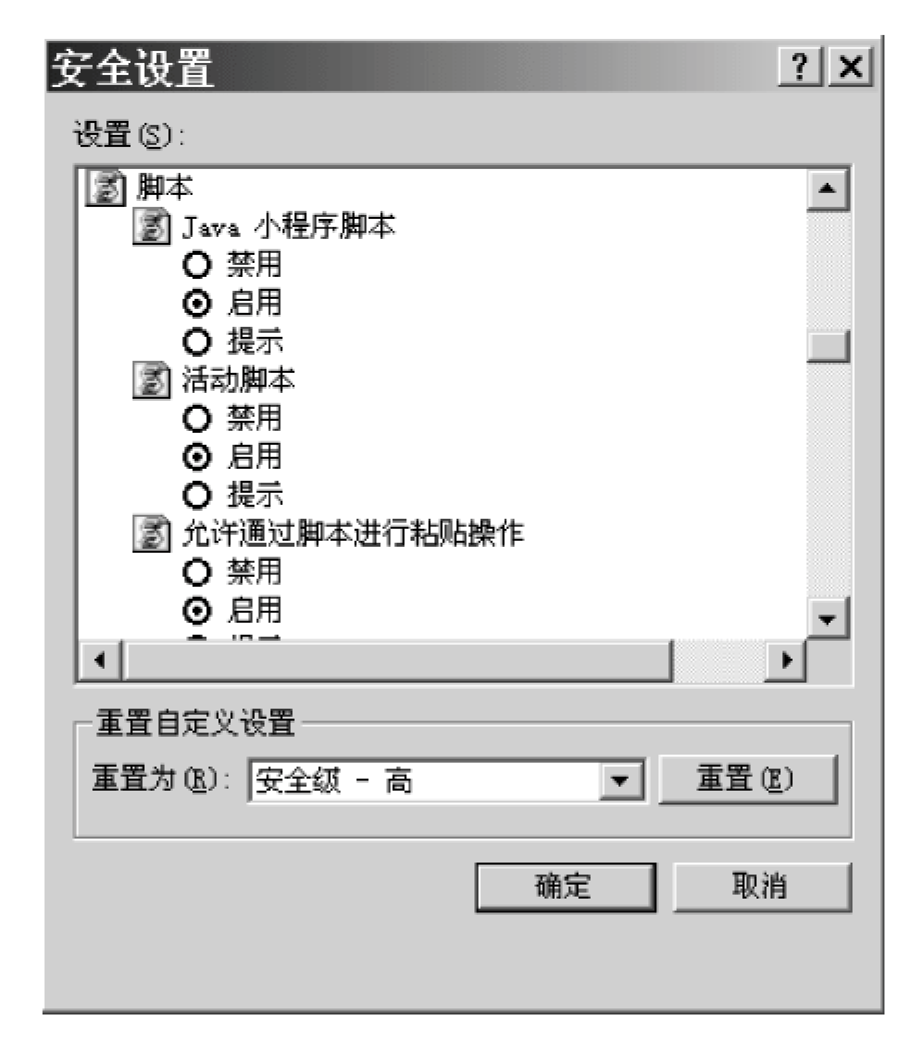


图 11-55　“安全设置”对话框

“https://192.168.31.3”访问企业 Web 站点，将弹出“选择数字证书”对话框，这时可以选择刚刚安装的客户证书。

⑨ 单击“查看证书”按钮，查看该证书的详细信息。该证书的目的是客户机向远程计算机(服务器)证明自己的身份。

⑩ 单击“确定”按钮，访问企业 Web 站点。

11.4.2 任务 2：构建高安全性的 FTP 服务器

1. 任务目标

对广大直面各种网络攻击的网络管理员、网络安全工程师来说，工作中必然会遇到各种各样的 FTP 攻击，如何在满足自己日常所需功能的前提下，构建一个方便、快捷并且安全性足够强的 FTP 服务器成为必须解决的问题。本任务主要完成使用 IIS FTP Server 构建可供网络管理员维护使用的 FTP 服务器，而且安全性足够高。

2. 工作任务

(1) 指定 FTP 的 IP 地址并修改默认端口；

(2) 定制详细的 FTP 日志，记录相关信息；

(3) 利用 NTFS 约束 FTP 用户权限；

(4) 启用目录安全性，杜绝 99%的各类 FTP 攻击。

3. 工作环境

一台预装 FTP 服务的 Windows Server 2003/XP 主机。

4. 实施过程

(1) 指定 FTP 的 IP 地址并修改默认端口

原则是使用专用 IP 进行 FTP 服务器搭建，使用足够隐蔽的端口进行通信。

① 在 FTP 建立向导的“IP 地址和端口设置”对话框进行如图 11-56 所示的设置。

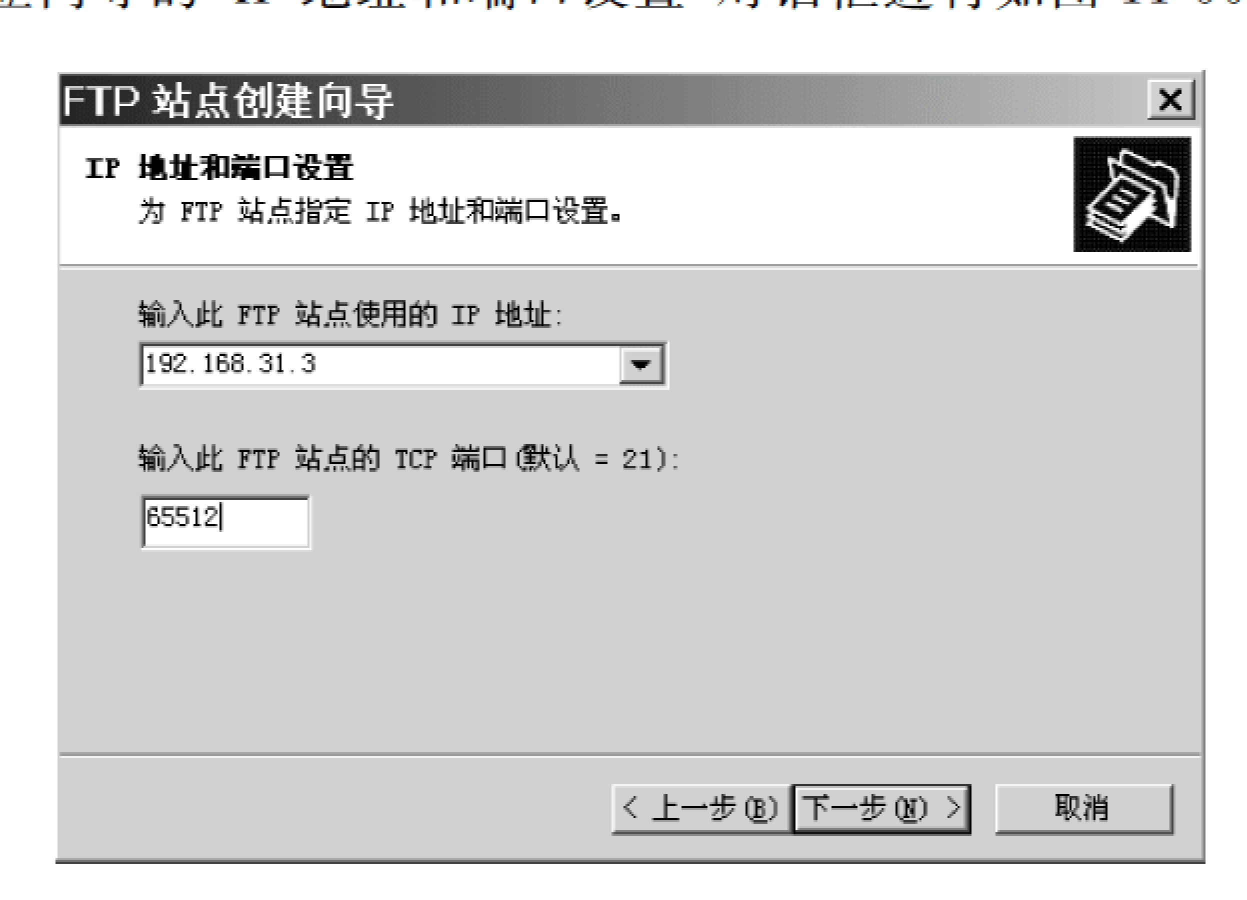


图 11-56 FTP 站点的 IP 地址和端口设置

注意：IP 地址不能选择“全部未分配”，应该尽量使用一个独立的、只为此 FTP 服务器提供的独特 IP 地址。这个 IP 地址没有公开，只有相关人员知道。这个 IP 地址可以用来使用 FTP 服务，也可以用来进行其他独特的服务器隐蔽管理。另外，使用足够隐蔽的端口进

行通信，端口设置建议不用默认端口，而是设置成一个大于 10000 且小于 65535 的数字，这是因为很多端口扫描工具默认情况下都不会扫描这部分端口，而攻击者如果手动设置扫描端口的话，出于时间和速度的考虑，也很少定义 1～65535 这样的端口扫描规则，所以很容易迷惑攻击者，让他们不知道还有一个高端端口在系统中发挥作用。

② 采用默认步骤，建立一个新的 FTP 服务器。

③ 在 CMD 命令提示符下使用“netstat -an”命令，可以看到系统中新开了一个端口，并且该端口正在监听，如图 11-57 所示。

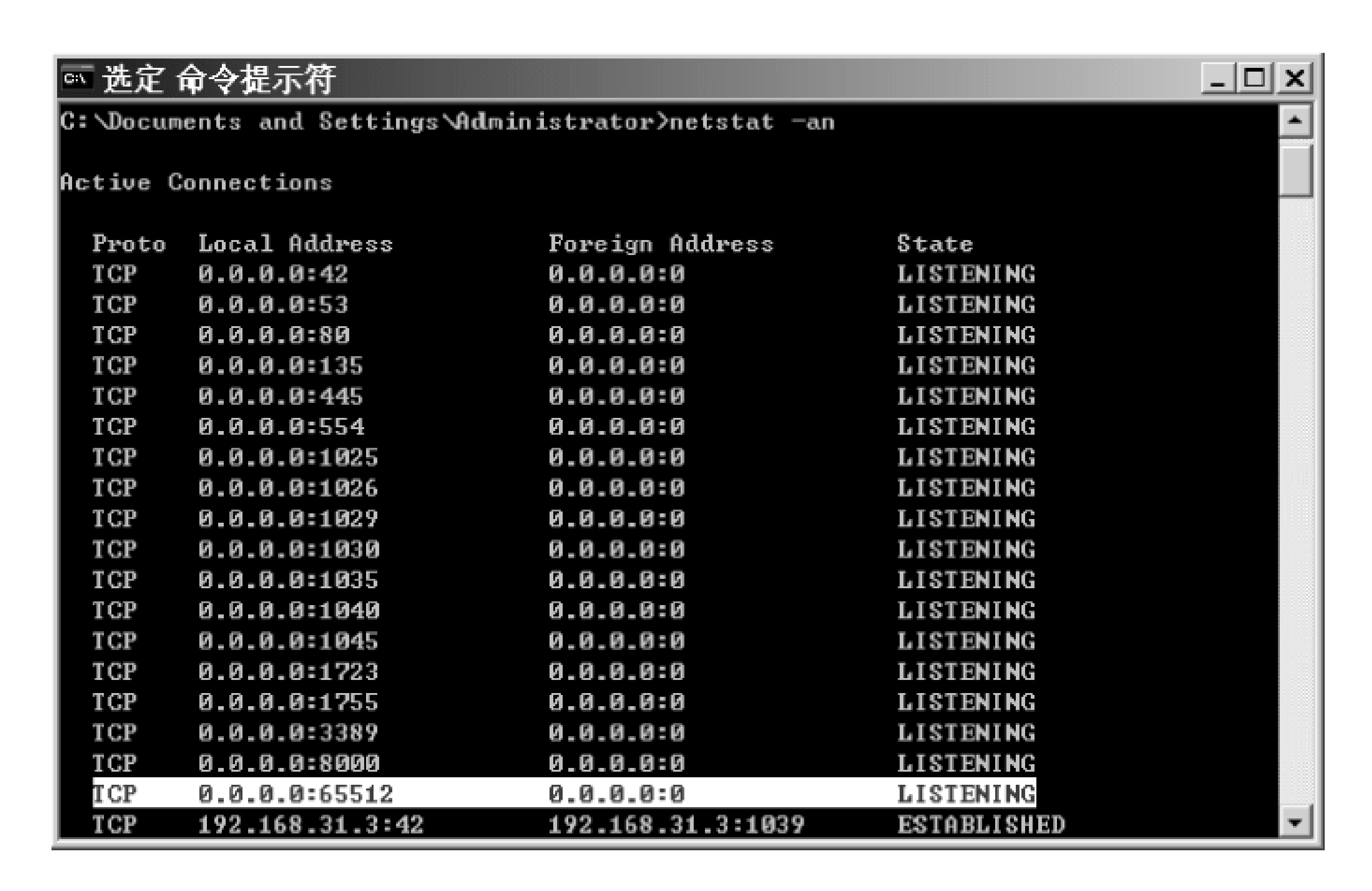


图 11-57　系统新开的端口

(2) 定制详细的 FTP 日志，记录相关信息

IIS 的 FTP 系统有非常完善、丰富的日志记录系统。使用日志系统来时刻记录 FTP 服务器的运行状态是非常重要的。

① 右击新建的 FTP 站点，在弹出的快捷菜单中选择“属性”按钮，界面如图 11-58 所示，可以看到 IIS 管理器下 FTP 站点中新建站点的 FTP 日志系统的默认设置情况。

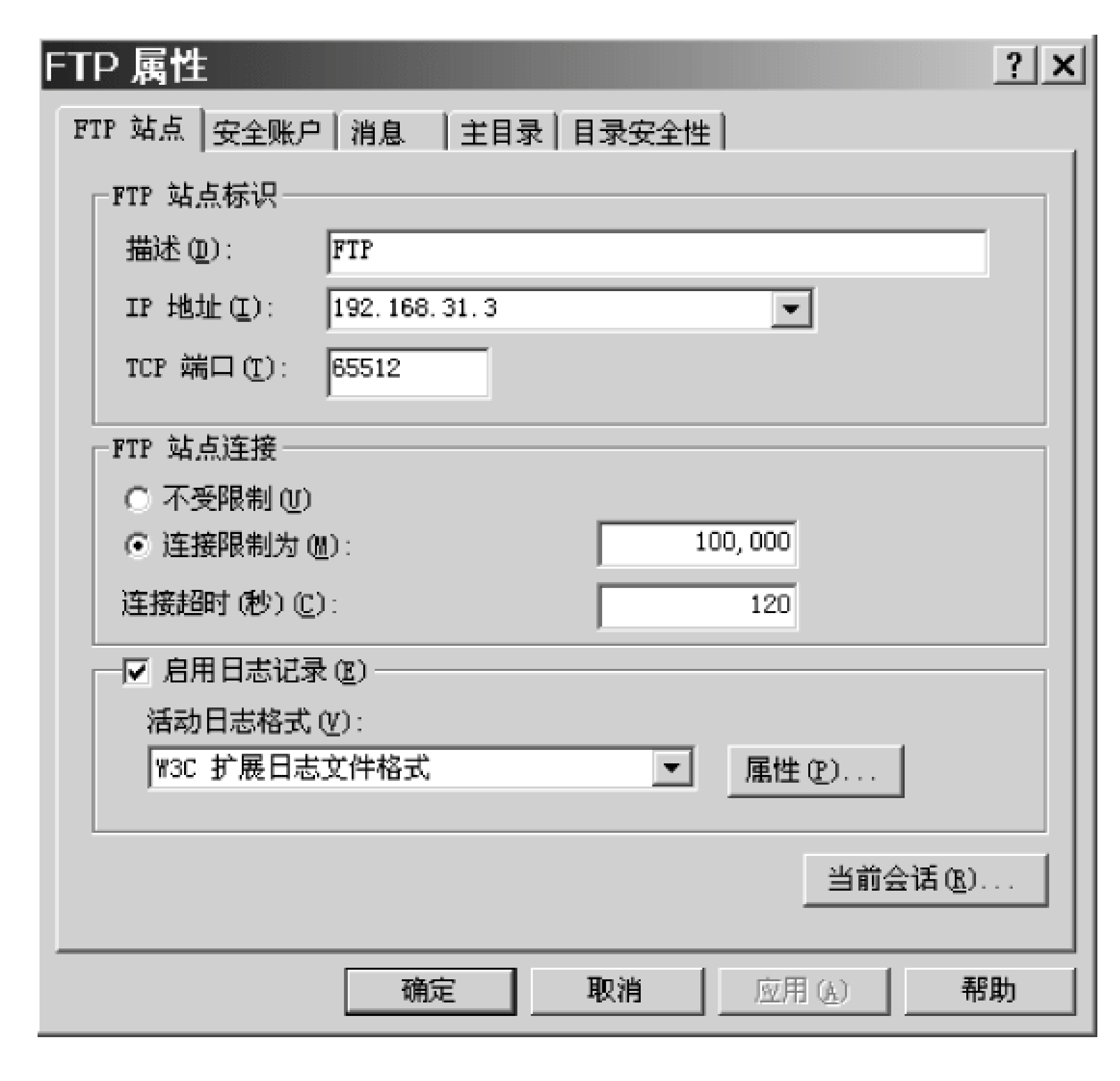


图 11-58　“FTP 属性”的“FTP 站点”选项卡设置

② 单击对话框中“启用日志记录”右侧的“属性”按钮，弹出“日志记录属性”对话框。选择“新日志计划”下的“当文件大小达到 20MB”时开始生成新的日志记录文件，设置“日志文件目录”到每个 FTP 用户单独使用的文件夹下，如图 11-59 所示。

“日志记录属性”设置是对日志系统进行详细的高级定义，定义的内容就是设置攻击者或者可能发生的攻击可能存在的典型特征。“新日志计划”控制每个日志文件的生成规则，默认是每天生成一份新的 FTP 日志。假如攻击者对某目标 FTP 服务器进行大规模分布式暴力破解攻击，如果 FTP 日志是按默认的记录方式记录，会产生无比庞大的单一文件，甚至可能达到几十 GB 的大小，导致系统运行出现问题。因此，选择“新日志计划”下的“当文件大小达到 20MB”时开始生成新的日志记录文件，以方便分析和调用。

“日志文件目录”也是非常重要的选项，定义 FTP 日志存放的地址，默认存放在“C:\WINDOWS\system32\LogFiles”下。事实上，对于任何被攻击者广泛了解的默认选项，都应该进行许可范围内的更改。正是出于对操作系统所在盘的保护，才更改“日志文件目录”。因此，设置“日志文件目录”到每个 FTP 用户单独使用的文件夹下，但不赋予该用户对此日志记录文件的访问权限。

③ 单击“日志记录属性”的“高级”选项卡，对扩展日志选项进行选择。一个设置好的日志系统记录信息如图 11-60 所示。



图 11-59 “日志记录属性”对话框的“常规”选项卡设置



图 11-60 “日志记录属性”对话框的“高级”选项卡设置

一个能记录绝大多数攻击者和使用者行为的日志文件应该包含以下信息：日期（非默认选中，需要手动选中）、时间（默认选中）、客户端 IP 地址（默认选中）、用户名（非默认选中，需要手动选中）、方法（默认选中）、URL 资源（默认选中）、协议状态（默认选中）、Win32 状态（默认选中）、所用时间（非默认选中，需要手动选中）和用户代理（非默认选中，需要手动选中）。

需要注意的是，并不是日志系统记录的信息越多越好。因为日志系统记录 FTP 用户（包括攻击者和正常用户）的访问毕竟需要消耗资源，而且生成的日志记录同样需要存放空间。如果记录项目过多，可能引起系统资源消耗大，日志文件占用空间大的问题。

(3) 利用 NTFS 约束 FTP 用户权限

使用 NTFS 文件系统时，必须为账户授予相应的 NTFS 权限，才能访问对应的文件或文件夹，可以在一定程度上保护数据的安全。

首先创建专用的 FTP 账户和对应的 FTP 文件夹，操作步骤如下：

① 假设有三名网络管理员需要对服务器进行经常性的维护，而且各自的工作职能不同，则在命令行下，使用如下命令建立三个专用的 FTP 账户，命令执行情况如图 11-61 所示。

```
Net user ftp01 Pass@001 /add
Net user ftp02 Pass@002 /add
Net user ftp03 Pass@003 /add
```

注意：受到组策略影响，创建的用户密码必须满足 8 位以上，包含大/小写字母、数字和特殊符号，否则创建账户将失败。

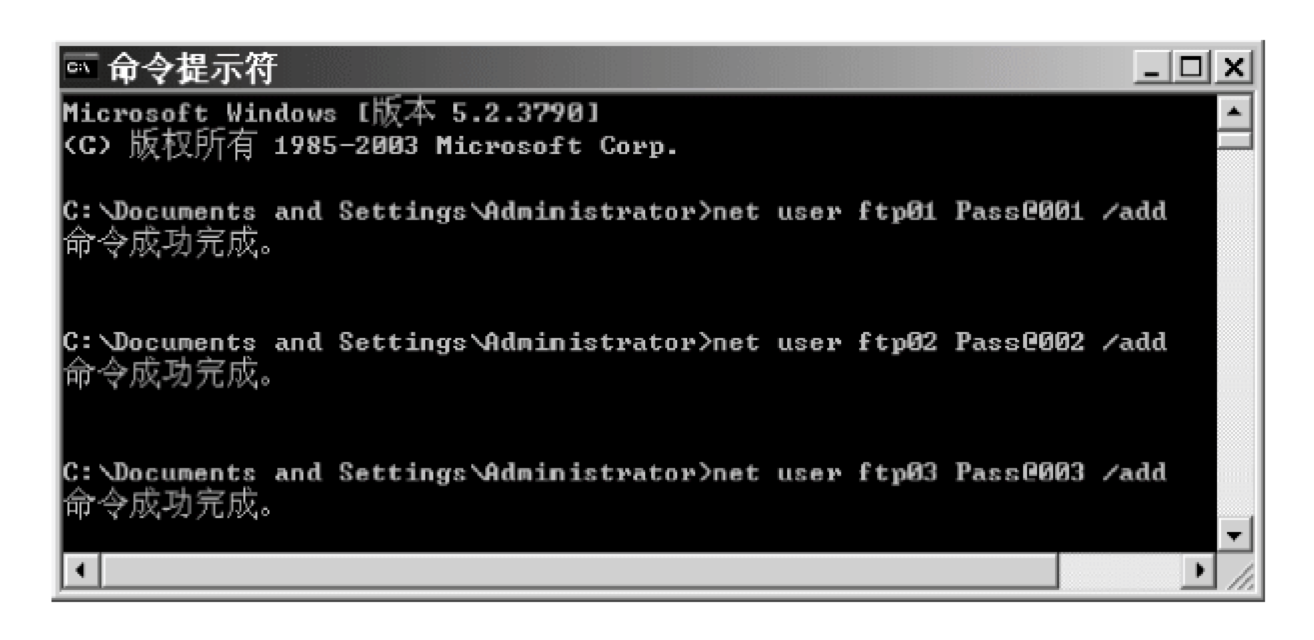


图 11-61　创建账户

② 使用"net user"命令创建的系统账户默认属于"user"组。利用"net"命令把这些账户从"user"组删除，并指派到"Guest"用户组。以 ftp01 账户为例，使用"net localgroup users ftp01 /del"命令删除"user"组权限，然后使用"net localgroup guests ftp01 /add"命令将该账户指派到"Guest"组。命令执行情况如图 11-62 所示。

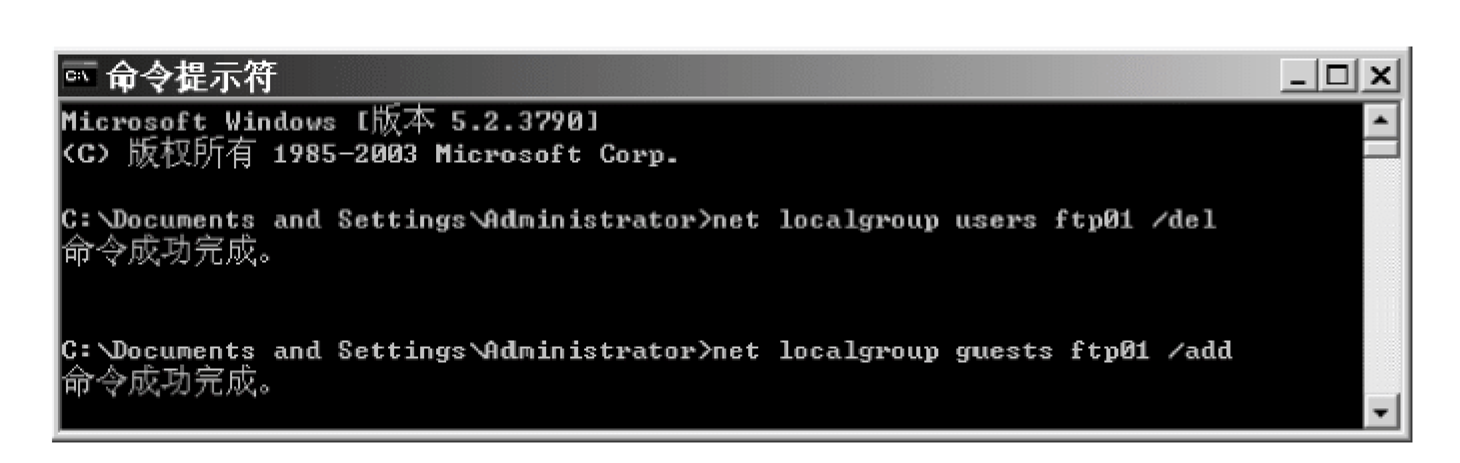


图 11-62　指派权限

③ 以系统管理员身份找到 FTP 的根文件夹，分别为每个用户创建一个对应的文件夹，同时建立各 FTP 用户的日志记录文件夹。例如，ftp01 账户对应的 FTP 文件夹是 d:\ftproot\01\ftp01，该账户的日志记录文件夹是 d:\ftproot\01\log01。日志文件夹的访问权限可以保留默认，或者添加日志记录必要的系统权限，只要 FTP 用户不能访问即可。

然后，利用 NTFS 约束 FTP 用户权限，具体操作如下：

① 选择"FTP 属性"对话框的"安全账户"选项卡，然后取消勾选"允许匿名连接"前的复选框，如图 11-63 所示。



图 11-63 “FTP 属性”对话框的“安全账户”选项卡设置

② 出现账户安全提示,如图 11-64 所示,单击“确定”按钮返回,则此时取消了 IIS 下 FTP 的匿名访问机制,所有登录 FTP 服务器的账户都需要系统指派。

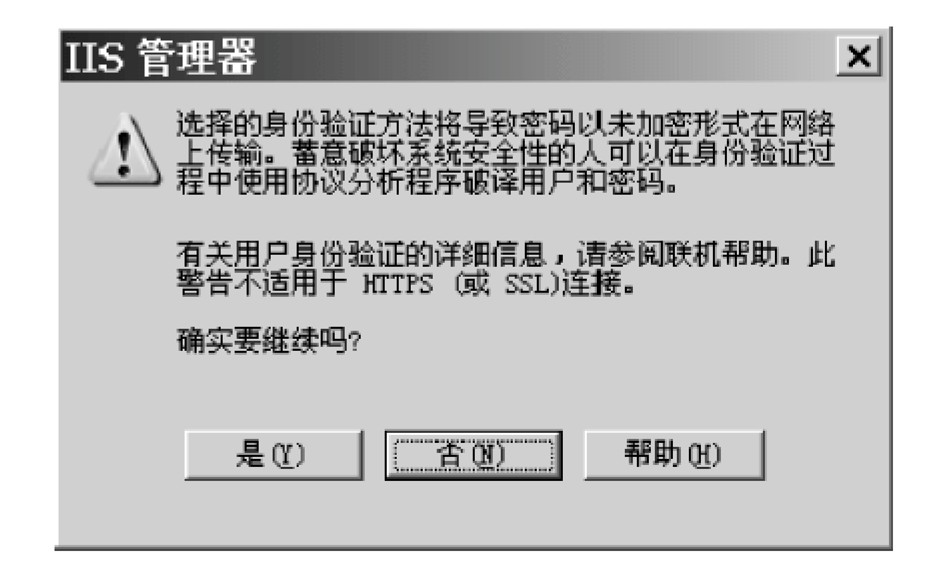


图 11-64 安全提示(2)

匿名访问是 IIS 下 FTP 服务器的默认设置。此设置可以很好地支持普通用户的 FTP 访问,但若要建立高安全性的 FTP 服务器,此项设置必须去除。

③ 选择“FTP 属性”对话框的“主目录”选项卡,更改 FTP 站点目录,如图 11-65 所示。

④ 利用组策略启用密码复杂性策略和密码最小值策略。

⑤ 选中 ftp01 文件夹,右击选择“安全”选项,弹出“ftp01 属性”对话框的“安全”选项卡。然后单击界面中的“添加”按钮,查找并选中 ftp01 账户,如图 11-66 所示。

图 11-65 “主目录”选项卡(2)



图 11-66 “安全”选项卡(2)

⑥ 默认情况下，这里有很多继承于上级文件夹的权限，需要删除这些默认权限。

以删除“SYSTEM”为例，选中“SYSTEM”，然后单击“删除”按钮，系统提示“因为SYSTEM 从其父系继承权限，您无法删除此对象，要删除‘SYSTEM’，您必须阻止对象继承权限。关闭继承权限的选项，然后重试删除‘SYSTEM’。”，如图 11-67 所示。

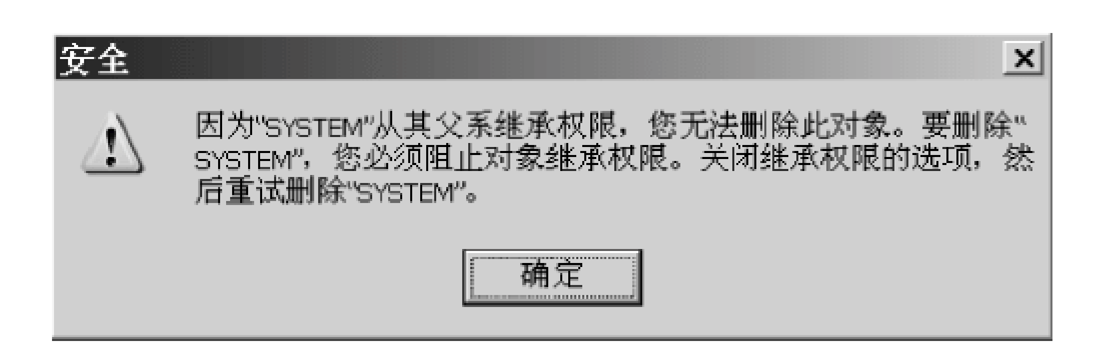


图 11-67　安全提示(3)

⑦ 单击“确定”按钮，然后单击“高级”按钮，弹出“高级安全设置”对话框，如图 11-68 所示。

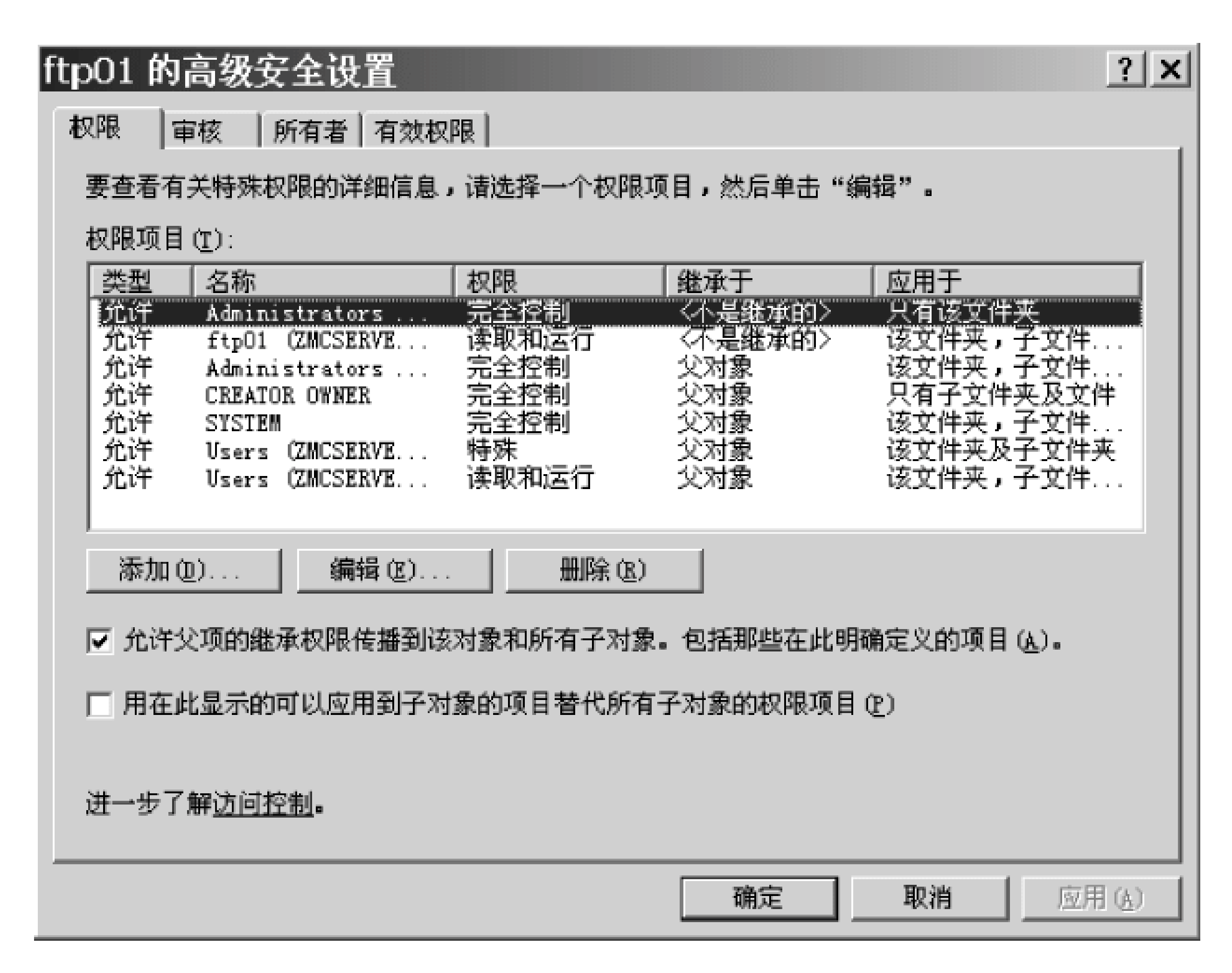


图 11-68　“高级安全设置”对话框

⑧ 去掉“允许父项的继承权限传播到该对象和所有子对象”前面的“√”，弹出如图 11-69 所示对话框。

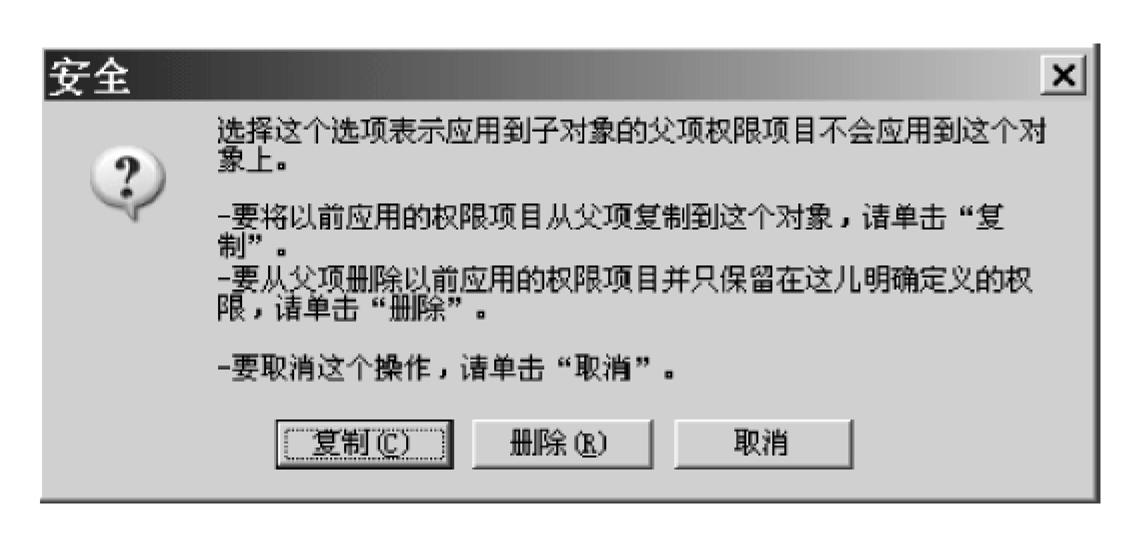


图 11-69　安全提示窗口

⑨ 单击“删除”按钮，删除残留在界面中的其他选项，然后单击“确定”按钮。此时，ftp01 默认拥有部分权限，包括“读取和运行”、“列出文件夹目录”、“读取”三种。因为网络管理员需要经常使用 FTP 的上传功能，因此选中“写入”权限。以 ftp01 账户为例，设置完成

后的界面如图 11-70 所示。

⑩ 单击“确定”按钮，此时远程登录 FTP 站点，会弹出“登录身份”对话框，如图 11-71 所示。



图 11-70 设置 ftp01 的权限

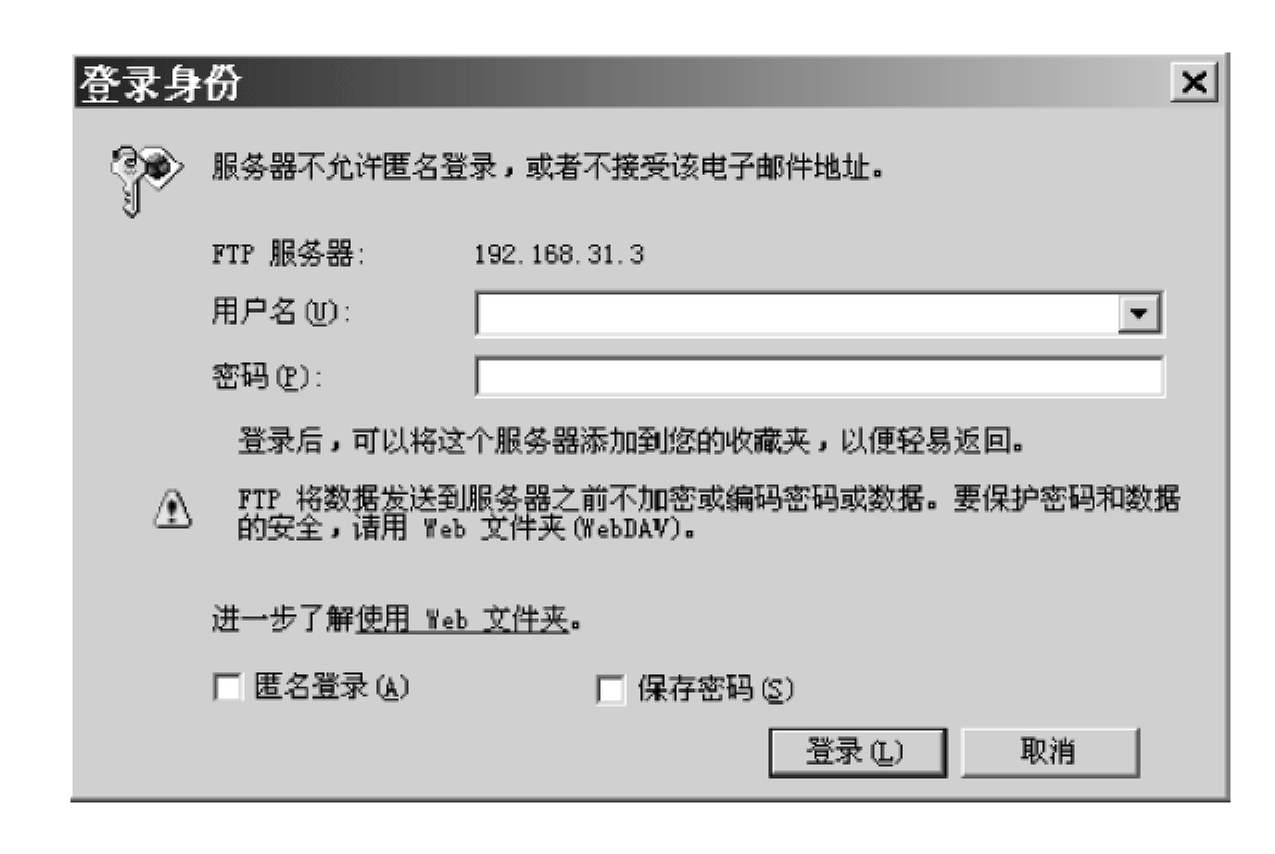


图 11-71 “登录身份”对话框

⑪ 输入账户 ftp01 的密码 Pass@001，登录到对应文件夹 ftp01，并能完成上传功能，如图 11-72 所示。若登录其他用户对应的文件夹，将弹出错误提示，如图 11-73 所示。

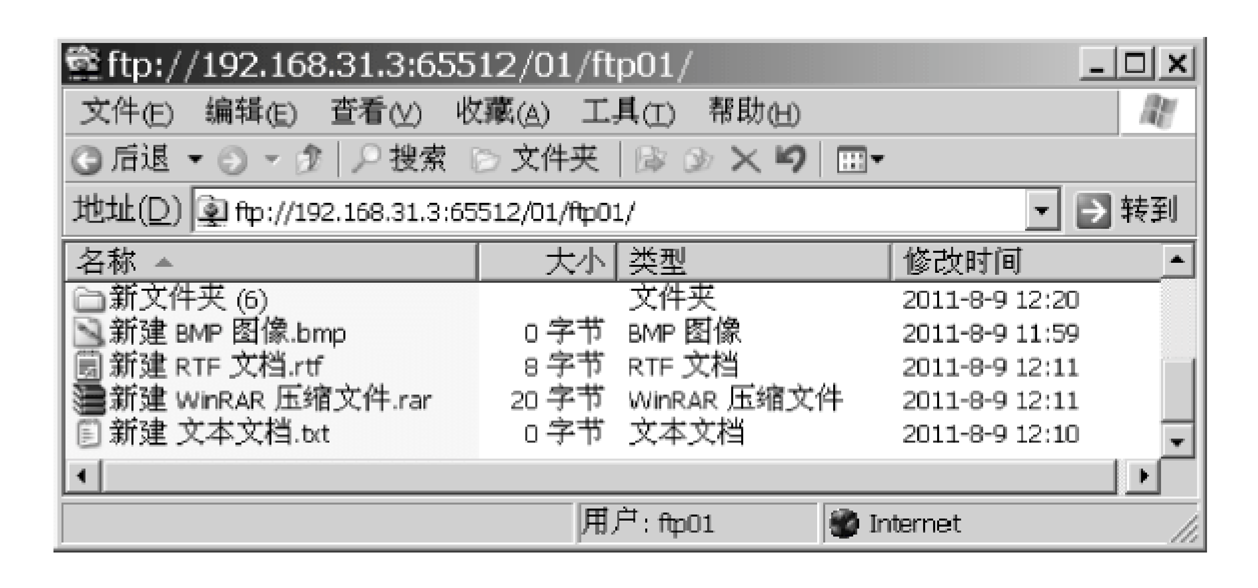


图 11-72 FTP 站点登录成功

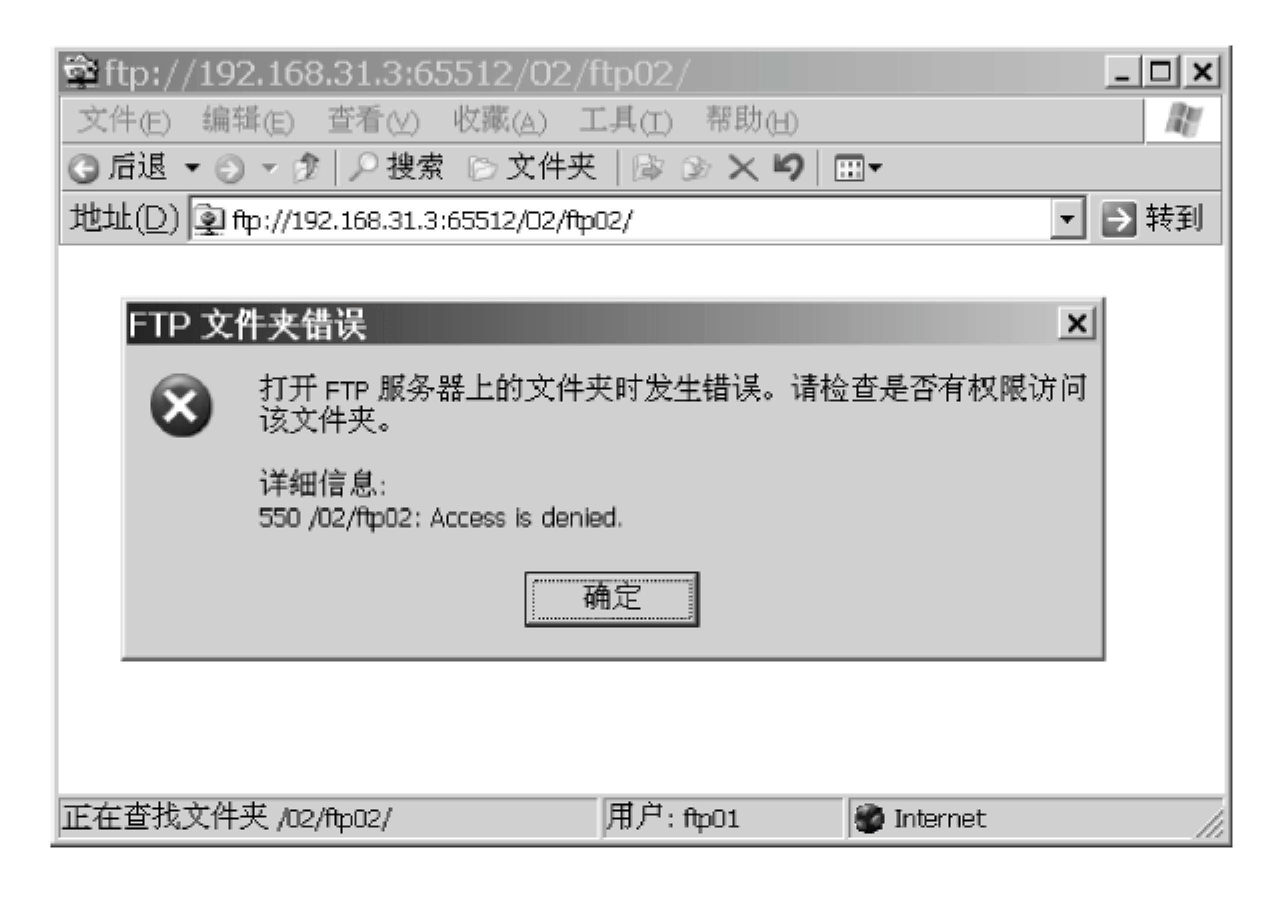


图 11-73 错误提示

⑫ 在 FTP 服务器的主机上，非 ftp01 用户都无法访问 ftp01 文件夹，如图 11-74 所示。



图 11-74　拒绝访问提示窗口

(4) 启用目录安全性，杜绝 99%的各类 FTP 攻击

如果攻击者即便得到 FTP 账户密码也没有登录权限，就能解决起码 99%以上的攻击。在 IIS 的 FTP Server 中，"目录安全性"可以实现这个功能，不过策略有些许变化，具体步骤如下：

右击 FTP 站点，然后选择"属性"项，打开"FTP 属性"对话框；选择"目录安全性"选项卡，在界面中选择"拒绝访问"，然后单击"添加"按钮，定义允许访问的单一计算机、多台计算机，设置好的界面如图 11-75 所示。



图 11-75　"目录安全性"设置

"目录安全性"是通过 FTP 用户登录的 IP 地址进行判断的一种机制。图 11-75 中的"拒绝访问"代表默认拒绝所有 IP 的 FTP 使用请求，除非请求登录 FTP 的计算机 IP 地址包含在"下面列出的除外"列表框中。通过这个设置，管理员可以控制唯一的，或者是极少的绝对信任 IP 可以使用 FTP 功能。

11.5　常见问题解答

在"安全通道"对话框中，"忽略客户端证书"、"接受客户端证书"和"要求客户端证书"三个单选按钮的区别是什么？

答：SSL 协议支持的是服务器端的认证，主要通过客户端对服务器端的数字证书进行认证，对客户端的认证是可选的，因此在"安全通信"对话框中有三个单选按钮供选择。三者的区别是："忽略客户端证书"是指服务器端不向客户端发送请求客户端证书的消息；"接受客户端证书"是指服务器端向客户端发送请求客户端证书的消息，但不要求客户端必须提供证书，即服务器端可以容忍客户不具备证书的情况；"要求客户端证书"是指服务器端向客户端发送请求客户端证书的消息，并强制要求客户端必须提供证书，否则通信将中断。如

果要求 Web 服务器既可以接收 HTTP 请求，也可以接收 HTTPS 请求，并要求客户端提供数字证书，需要选中“接受客户端证书”单选按钮，注意不要选中“要求安全通道(SSL)”复选框。如果 Web 服务器管理员希望 Web 服务器只接收 HTTPS 请求，并要求客户 IE 浏览器和 Web 服务器之间实现 128 位加密，并且不要求客户端提供数字证书，需要选中“要求安全通道(SSL)”复选框，选中“要求 128 位加密”复选框，并选中“忽略客户端证书”单选按钮。如果选中“要求安全通道(SSL)”复选框，并选中“要求客户端证书”单选按钮，那么 Web 服务器将对客户端证书进行强制认证。

11.6 过关练习

一、选择题

1. 以下用于在网络应用层和传输层之间提供加密方案的协议是(　　)。

A. PGP　　B. SSL　　C. IPSec　　D. DES

2. 某 Web 网站向 CA 申请了数字证书。用户登录该网站时，通过验证(　　)，可确认该数字证书的有效性，从而(　　)。

(1) A. CA 的签名　B. 网站的签名　C. 会话密钥　D. DES 密码

(2) A. 向网站确认自己的身份　B. 获取访问网站的权限

C. 和网站进行双向认证　D. 验证该网站的真伪

3. (　　)不属于 PKI CA(认证中心)的功能。

A. 接受并验证最终用户数字证书的申请

B. 向申请者颁发或拒绝颁发数字证书

C. 产生和发布证书废止列表(CRL)，验证证书状态

D. 业务受理点 LRA 的全面管理

4. 为保障 Web 服务器的安全运行，对用户要进行身份验证。关于 Windows Server 2003 中的“集成 Windows 身份验证”，下列说法错误的是(　　)。

A. 在这种身份验证方式中，用户名和密码在发送前要经过加密处理，所以是一种安全的身份验证方案

B. 这种身份验证方案结合了 Windows NT 质询/响应身份验证和 Kerberos V5 身份验证两种方式

C. 如果用户系统在域控制器中安装了活动目录服务，而且浏览器支持 Kerberos V5 身份认证协议，则使用 Kerberos V5 身份验证

D. 客户机通过代理服务器建立连接时，可采用集成 Windows 身份验证方案进行验证

5. 实现保密通信的 SSL 协议工作在 HTTP 层和(　　)层之间。SSL 加密通道的建立过程如下：首先，客户端与服务器建立连接，服务器把它的(　　)发送给客户端；客户端随机生成(　　)，并用从服务器得到的公钥对它进行加密，通过网络传送给服务器；服务器使用(　　)解密得到会话密钥，客户端和服务器端就建立了安全通道。

A. TCP　　B. IP　　C. UDP　　D. 公钥

E. 私钥　　F. 对称密钥　　G. 会话密钥　　H. 数字证书

I. 证书服务

6. 在安装 SSL 时，在“身份验证方法”对话框中应选用的登录验证方式是(　　)。

A. 匿名身份验证　　B. 基本身份验证

C. 集成 Windows 身份验证　　D. 摘要式身份验证

7. 若 FTP 服务器开启了匿名访问功能，匿名登录时需要输入的用户名是(　　)。

A. root　　B. user　　C. guest　　D. anonymous

二、填空题

SSL 协议使用________密钥体制进行密钥协商。在 IIS 6.0 中，Web 服务器管理员必须先安装 Web 站点证书，Web 服务器才能支持 SSL 会话。通常，数字证书由________颁发，其格式遵循 ITU-T ________标准。

三、简答题

IIS 服务器安全设置的方法有哪些？

学习情境三

企业网中主要网络设备的安全配置

学习情境三主要介绍企业网中主要网络设备的安全配置，以及主流网络安全设备的配置和管理，包括交换机、路由器、网络防火墙、入侵检测系统 IDS、VPN 服务器等产品的基本配置、基本界面和功能配置。学生通过 5 个工作任务的训练，掌握最常用的网络设备交换机和路由器的安全配置；熟悉防火墙的部署与配置；利用入侵检测系统 IDS 进行事件查询和报表查看的方法，自定义规则和关联规则的作用和配置方式；正确配置 VPN 服务器，并采用正确方法对 VPN 连接结果进行检查。

通过本单元所有任务的实践，可以学会如何对企业网网络设备进行安全部署，解决网络安全设备配置中遇到的问题。

本学习情境需要完成的工作任务如下：

工作任务十二　设置企业网中交换机安全
工作任务十三　设置企业网中路由器安全
工作任务十四　防火墙的配置与应用
工作任务十五　入侵检测系统 IDS 的部署与配置
工作任务十六　VPN 服务器的配置与管理

工作任务十二

设置企业网中交换机安全

12.1 用户需求与分析

交换机的主要功能是提供网络数据包优化和转发，存在被攻击或入侵的危险。一旦入侵者得到交换机的控制权限，所有通过该交换机转发的数据包都将受到威胁。通常情况下，网络安全管理员可以通过配置端口传输控制、端口认证、ARP 检测、创建 VLAN 等措施加强交换机的安全性。

12.2 预 备 知 识

1. 在交换机上实现访问控制列表

访问控制列表（Access Control List，ACL）是一种访问控制技术，被广泛应用于三层交换机和路由器。借助 ACL 可以有效控制用户对网络和 Internet 的访问，从而最大限度地保障网络安全。

交换机支持三种访问控制列表的应用过滤传输，可以在同一交换机上实施端口访问列表、路由访问列表和 VLAN 访问列表，端口访问列表优先于路由访问列表和 VLAN 访问列表。可以根据网络管理员指定的访问控制准则来控制端口对数据包的接收和拒绝。

访问列表的类型有三种：标准 IP 访问列表、扩展 IP 访问列表和命名访问控制列表。

标准 IP 访问列表只允许过滤源地址，根据源网络、子网或主机的 IP 地址来决定对数据包的过滤，且功能十分有限。当阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者拒绝某一协议簇的所有通信流量时，可以使用标准 IP 访问控制列表来实现。标准访问控制列表检查路由器的数据包的源地址，从而允许或拒绝基于网络、子网或主机的 IP 地址的所有通信流量通过三层设备的出口。

扩展 IP 访问控制列表允许过滤源地址、目的地址和上层应用数据，因此可以适应各种复杂的网络应用。扩展 IP 访问控制列表既检查数据包的源地址，也检查数据包的目的地址，还检查数据包的特定协议类型、端口号等。扩展 IP 访问控制列表具有灵活性和扩充性，针对某一地址，允许使用某些协议的通信流量通过，而拒绝使用其他协议的流量通过。

在标准与扩展 IP 访问控制列表中均要使用表号，而在命名访问控制列表中使用一个字母或数字组合的字符串来代替这些数字。使用命名访问控制列表可以删除某一特定的控制条目，这样，可以在使用过程中方便地进行修改。

配置访问控制列表的具体步骤是：定义一个标准(或扩展)的访问控制列表；为访问控制列表配置包过滤的准则；配置访问控制列表的应用接口。

2. 基于端口的传输控制

在局域网安全架构中，交换机安全是非常重要的，在整个内网安全体系中起了决定性的作用。目前大多数局域网中都配有三层交换机，安全功能非常丰富，通过合理配置，与网络防火墙协同工作，成为网络安全的又一道屏障。借助对端口传输控制的配置，既可以有效杜绝广播风暴对整个网络的冲击，从而保证网络的正常通信；又可以拒绝未被授权的计算机接入网络，或者限制某个接口接入计算机的数量，从而保证网络的接入安全，避免网络被个别用户滥用。

当端口收到大量的广播、单播或多播包时，会发生广播风暴。转发这些包将导致网络速度变慢或超时。借助于对端口的广播风暴控制，可以有效避免硬件损坏或链路故障而导致的网络瘫痪。默认情况下，广播、多播和单播风暴控制被禁用，需要时可将其开启。

流控制只适用于 1000Base-T、1000Base-SX、10GBase-FX 和 GBIC 端口。在千兆端口启用流控制后，可以在拥塞期间暂停其他终端的连接。当端口处于拥塞状态，无法接收到数据流时，将通知其他接口暂停发送，直到恢复正常状态。当本地设备发现任何终端发生拥塞时，将发送一个暂停帧，以通知其连接伙伴或远端拥塞设备。当收到暂停帧后，远程设备将停止发送任何数据包，以防止在拥塞期内丢失任何数据包。

保护端口可以确保同一交换机上的指定端口之间不进行通信。保护端口不向其他保护端口转发任何传输，包括单播、多播和广播包。传输不能在第二层保护端口间进行，所有保护端口间的传输都必须通过第三层设备转发。保护端口与非保护端口间的传输不受任何影响。

默认状态下，未知目的 MAC 地址的广播包被允许从端口向外传输。如果未知的单播和多播通信被转发到保护端口，将导致安全问题。可以采用阻塞端口的方式，以防止未知的单播和多播通信在端口间转发。

12.3 方案设计

方案设计如表 12-1 所示。

表 12-1 方案设计

任务名称	设置企业网中交换机安全
任务分解	1. IP 访问列表的设置 (1) 创建标准访问列表 (2) 创建扩展访问列表 (3) 创建标准 IP 访问列表名称 (4) 创建扩展 IP 访问列表名称 2. 基于端口的传输控制 (1) 风暴控制 (2) 流控制 (3) 保护端口 (4) 端口阻塞

续表

能力目标	1. 能在交换机上创建标准访问控制列表 2. 能在交换机上创建扩展访问控制列表 3. 能使用网络监听工具查看攻击效果 4. 能对分布式拒绝服务攻击工具 DDoS 攻击者的攻击属性进行设置 5. 能使用分布式拒绝服务攻击工具 DDoS 对目标主机发动拒绝服务攻击
知识目标	1. 熟悉访问控制列表的作用 2. 了解访问控制列表的分类 3. 了解基于端口访问控制的原理
素质目标	1. 树立较强的安全意识 2. 培养吃苦耐劳、实事求是、一丝不苟的工作态度 3. 培养分析能力和应变能力 4. 具有可持续发展能力 5. 了解网络安全行业的基本情况

12.4　任务实施

12.4.1　任务 1：IP 访问列表的设置

1. 任务目标

借助 ACL 有效控制用户对网络和 Internet 的访问，从而最大限度地保障网络安全。

2. 工作任务

(1) 创建标准访问列表；

(2) 创建扩展访问列表；

(3) 创建标准 IP 访问列表名称；

(4) 创建扩展 IP 访问列表名称。

3. 工作环境

(1) 一台预装 Windows Server 2003/XP 的主机。

(2) 一台交换机。

4. 实施过程

(1) 创建标准访问列表

① 输入“configure terminal”进入全局配置模式。

② 使用源地址或通配符定义标准 IP 访问列表，格式如下：

```
access-list access-list-number {deny|permit} source [source-wildcard]
```

- access-list-number 是 ACL 号，又称为表号，用来标识或引用访问控制列表。表号用数字表示。ACL 号相同的所有 ACL 形成一个组。在判断一个包时，使用同一组中的条目从上到下逐一判断，一旦遇到满足条件的条目，就终止对该包的判断。标准访问控制列表的表号范围是 1～99 或 1300～1999。

- deny|permit：当条件匹配时，是允许包通过，还是将包丢弃。
- source：源地址，发送包的网络或主机地址，使用通配符屏蔽码表示一组主机。
- source-wildcard：通配符屏蔽码，实际上就是子网掩码的反码。
- any：表示任何主机。

访问控制列表是一个连续的列表，至少由一个“permit(允许)”语句和一个或多个“deny(拒绝)”语句构成。在配置过滤规则时，特别要注意 ACL 语句的顺序。因为数据包只有在前一个判断条件不匹配时才交给 ACL 中的下一个条件语句进行比较。

例如，若要拒绝从源地址 192.168.1.100 发出的报文，但允许发自其他源地址的报文，应当使用下列指令：

```
access-list 1 deny host 192.168.1.100
access-list 1 permit any
```

注意两条语句的顺序。访问列表语句的处理顺序是从上到下，如果把两句颠倒，则不能过滤来自主机的报文，因为 permit 语句将允许所有的报文通过。

若要允许从 192.168.1.200 发出的报文，则使用下列指令：

```
access-list 1 permit 192.168.1.200 0.0.0.0
```

也可以用下面的语句代替：

```
access-list 1 permit host 192.168.1.200
```

③ 使用“end”返回特权配置模式。

(2) 创建扩展访问列表

标准 IP 访问列表只能控制源 IP 地址，不能控制端口。若要控制企业用户的网络应用，需要使用扩展 IP 访问列表。扩展访问控制列表可以检查数据包的源 IP 地址、目的 IP 地址、指定的协议、端口号等，以决定对数据包的过滤。

① 输入“configure terminal”进入全局配置模式。

② 定义扩展 IP 访问列表，表号取值范围为 100～199 或 2000～2699。

```
access-list access-list-number {deny | permit} protocol source source-wildcard [operator port]
destination destination-wildcard [operator port]
```

或者

```
access-list access-list-number {deny|permit} protocol any [operator port] any [operator port]
```

或者

```
access-list access-list-number {deny|permit} protocol host source [operator port] host destination
[operator port]
```

- protocol：要过滤的协议，例如 IP、TCP、UDP 和 ICMP 等。默认过滤所有协议。若要根据特殊协议进行报文过滤，需指定协议。
- destination destination-wildcard：目的地址和通配符屏蔽码。
- operator：端口操作符，在协议类型为 TCP 或 UDP 时支持端口比较，支持的比较操作有等于(eq)、大于(gt)、小于(lt)、不等于(neq)或介于(range)。若操作符为 range，后面需要跟两个端口。

例如，若要允许来自所有地址的包含有 SMTP 数据的报文到达 192.168.10.10 主机，可以在访问列表中添加下列指令：

```
access-list 101 permit tcp any host 192.168.10.10 eq smtp
```

③ 使用“end”命令返回特权配置模式。

(3) 创建标准 IP 访问列表名称

命名 IP 访问列表有两个优点，一是可以解决 ACL 号码不足的问题；二是可以自由地删除 ACL 中的一条语句，而不必删除整个 ACL。缺点是无法实现在任意位置加入新的 ACL 条目。

① 输入“configure terminal”命令进入全局配置模式。

② 利用名称定义标准 IP 访问列表，进入访问列表配置模式。名称可以是 1～99。

```
ip access-list standard name
```

③ 定义一个或多个 permit 或 deny 条件，以确定对包实时转发或是丢弃。

```
deny {source [source-wildcard]|host source |any}
```

或者

```
permit {source [source-wildcard]|host source |any}
```

④ 使用“end”返回特权配置模式。

例如，创建一条 IP Standard Access-list，该 ACL 名字为 deny-host192.168.12.x。有两条 ACE，第一条 ACE 拒绝来自 192.168.12.0 网段的任一主机，第二条 ACE 允许其他的任意主机。

```
ip access-list standard deny-host 192.168.12.x
deny 192.168.12.0 0.0.0.255 any
permit any
end
show access-list
```

(4) 创建扩展 IP 访问列表名称

① 使用“configure terminal”进入全局配置模式。

② 利用名称定义扩展 IP 访问列表，进入访问列表配置模式。名称可以是 100～199。

```
ip access-list extended name
```

③ 定义一个或多个 permit 或 deny 条件，以确定对包实施转发或是丢弃。

```
{deny | permit} protocol {source [source-wildcard] | host source | any} {destination [destination-wildcard] | host destination |any}
```

④ 利用“end”命令返回特权配置模式。

例如，创建一条 Extended IP ACL，该 ACL 有一条 ACE，用于允许指定网络(192.168.x.x)的所有主机以 HTTP 访问服务器 172.168.12.3，但拒绝其他所有主机使用网络。

```
ip access-list extended allow_oxc0a800_to_172.168.12.3
```

```
permit tcp 192.168.0.0 0.0.255.255 host 172.168.12.3 eq www
show acess-list
```

例如，借助扩展 IP 访问列表，可以在 VLAN 或端口上阻止蠕虫端口，从而避免蠕虫在网络中的蔓延，以保证网络的传输效率。

```
access-list 110 deny tcp any any range 135 139
access-list 110 deny tcp any any eq 445
access-list 110 deny tcp any any eq 593
access-list 110 deny tcp any any eq 1029
access-list 110 deny tcp any any eq 4444
access-list 110 deny tcp any any eq 5000
access-list 110 deny tcp any any eq 5554
access-list 110 deny tcp any any eq 7955
access-list 110 deny udp any any range 135 139
access-list 110 deny udp any any eq tftp
access-list 110 deny udp any any range 995 999
access-list 110 deny udp any any eq 1434
access-list 110 deny tcp any any gt 8090
access-list 110 deny udp any any eq 8090
access-list 110 permit ip any any
```

然后，将该访问列表应用至端口或 VLAN，在入和出双向上启用该列表。

```
ip access-group 110 in
ip access-group 110 out
```

例如，将 access-list deny_unknow_device 应用于 10/100Mb/s 接口 2 上：

```
interface fastethernet 0/2
ip access-list deny_unknow_device in
```

12.4.2 任务 2：基于端口的传输控制

1. 任务目标

借助对端口传输控制的配置，杜绝广播风暴对整个网络的冲击，从而保证网络的正常通信；同时启用流控制，在拥塞期间暂停终端的连接，直到恢复正常状态，以保证网络的正常通信；还可以拒绝未被授权的计算机接入网络，或者限制某个接口接入计算机的数量，保证网络的接入安全，避免网络被个别用户滥用。

2. 工作任务

(1) 风暴控制；

(2) 流控制；

(3) 保护端口；

(4) 端口阻塞。

3. 工作环境

(1) 一台预装 Windows Server 2003/XP 的主机。

(2) 一台交换机。

4. 实施过程

(1) 风暴控制

① 输入“configure terminal”进入全局配置模式。

② 指定欲配置的接口,进入接口配置模式。

```
interface interface-id
```

③ 配置广播、多播或单播风暴控制。默认状态下,风暴控制被禁用。通常情况下,应当启用广播风暴控制。

```
storm-control {broadcast|multicast|unicast} level {level [level-low] |bps bps [bps-low]| pps pps
[pps-low]}
```

- level 指定阻塞端口的带宽上限值,取值范围为 0～100。如果将值设为 100%,将不限制任何传输;如果设为 0%,那么该端口所有的广播、多播和单播都被阻塞。建议取值在 30%左右。
- level-low 指定启用端口的带宽下限值。端口带宽应当小于或等于下限值。当广播、多播和单播传输占用带宽的比例低于该值时,端口恢复转发,取值范围为 0～100。建议取值在 20%左右。
- bps 指定端口阻塞的传输速率上限值。当广播、多播或单播传输达到每秒若干比特(bps)时,端口将阻塞传输。建议取值范围不高于端口速率的 1/3～1/2。
- bps-low 指定端口阻塞的传输速率下限值。传输速率应当小于或等于下限值。当广播、多播或单播传输低于每秒若干比特(bps)时,端口将恢复传输。建议取值范围不高于端口速率的 1/3～1/2。如果数值较大,也可以使用 K、M 或 G 等单位表示。
- pps 指定端口阻塞的转发速率上限值。当广播、多播或单播传输速率达到每秒若干包(pps)时,端口将阻塞传输。建议取值范围不高于端口转发速率的 1/3～1/2。
- pps-low 指定端口启用的传输速率下限值。传输速率应当小于或等于下限值。当广播、多播或单播转发速率低于每秒若干包(pps)时,端口将恢复传输。建议取值范围不高于端口转发速率的 1/3～1/2。如果数值较大,也可以使用 K、M 或 G 等单位表示。

④ 指定风暴发生时如何处理。默认情况下,将过滤外出的传输,并不发送 SNMP 陷阱。当风暴发生时,应当选择 shutdown 该端口,避免由此导致网络瘫痪。

```
storm-control action {shutdown|trap}
```

⑤ 输入“end”返回特权模式。

(2) 流控制

① 输入“configure terminal”进入全局配置模式。

② 指定欲配置的接口,进入接口配置模式。

```
interface interface-id
```

③ 设置端口的流控制。

flowcontrol {receive|send} {on|off|desired}

④ 输入“end”返回特权配置模式。

⑤ 显示接口状态。

show interfaces interface-id

(3) 保护端口

① 输入“configure terminal”进入全局配置模式。

② 指定欲配置的接口,进入接口配置模式。

interface interface-id

③ 将接口配置为保护端口。

flowcontrol {receive|send} {on|off|desired}

④ 输入“end”返回特权配置模式。

⑤ 显示接口状态。

show interfaces interface-id switchport

(4) 端口阻塞

① 输入“configure terminal”进入全局配置模式。

② 指定欲配置的接口,进入接口配置模式。

interface interface-id

③ 禁止未知多播从该端口向外传输。

switchport block multicast

④ 禁止未知单播从该端口向外传输。

switchport block unicast

⑤ 输入“end”返回特权配置模式。

⑥ 显示接口状态。

show interfaces interface-id switchport

12.5 常见问题解答

访问列表的配置步骤是什么?

答:①分析需求,确定需要保护或控制的对象,为方便配置,最好以表格形式列出;②分析符合条件的数据流的路径,寻找一个最适合进行控制的位置;③编写 ACL,并将 ACL 应用到接口上;④测试并修改 ACL。

12.6 过关练习

一、选择题

1. 网络隔离技术的目标是确保把有害的攻击隔离,在保证可信网络内部信息不外泄的前提下,完成网络间数据的安全交换。下列隔离技术中,安全性最好的是(　　)。

A. 多重安全网关　　B. 防火墙　　C. VLAN 隔离　　D. 物理隔离

2. 通过交换机连接的一组工作站(　　)。

A. 组成一个冲突域,但不是一个广播域

B. 组成一个广播域,但不是一个冲突域

C. 既是一个冲突域,又是一个广播域

D. 既不是冲突域,也不是广播域

3. 访问控制列表(ACL)分为标准和扩展两种。下面关于 ACL 的描述中,错误的是(　　)。

A. 标准 ACL 可以根据分组中的 IP 源地址进行过滤

B. 扩展 ACL 可以根据分组中的 IP 目标地址进行过滤

C. 标准 ACL 可以根据分组中的 IP 目标地址进行过滤

D. 扩展 ACL 可以根据不同的上层协议信息进行过滤

二、填空题

访问列表的三种类型是________、________和________。

三、简答题

创建扩展访问列表的步骤是什么?

四、实操题

写出将接口配置为保护端口的命令。

工作任务十三

设置企业网中路由器安全

13.1 用户需求与分析

用户希望能利用企业现有路由器配置访问控制列表 ACL 和网络地址转换 NAT 等功能，在尽可能最小的经济投入下实现对企业网络的基本防护。对学习情境中企业常见网络设备路由器进行基本防火墙功能的配置，这是多数企业所采取的基本保护方式。

13.2 预 备 知 识

1. 在路由器上实现访问控制列表

当需要在路由器上对进出企业内部网络的协议数据进行过滤和控制时，可以采用路由器中的访问控制列表技术来配置过滤规则。访问控制列表(Access Control List，ACL)在思科路由器上常用的有两类：标准访问控制列表和扩展访问控制列表。

标准访问控制列表的格式为

```
access-list listnumber {permit|deny} address [wildcard-mask]
```

此格式表示允许或拒绝来自指定网络的数据包，该网络由 IP 地址(address)和地址通配比较位(wildcard-mask)指定。在思科路由器中，访问控制列表仅对源地址进行检查。标准访问列表的例子如下：

```
access-list 10 deny 192.168.31.0 0.0.0.255
```

表示该规则序号为 10，禁止来自源地址 192.168.31.0 的访问。

```
access-list 10 permit host 192.168.31.3
```

表示该规则序号为 10，允许来自 192.168.31.3 的主机的访问。

扩展访问控制列表格式为

```
access-list listnumber {permit|deny} protocol source source-wildcard-mask destination destination-wildcard-mask [operator operand] [log]
```

此格式表示允许或拒绝指定协议，源自指定网络、指定端口号、指定目的地址、指定目的端口的数据包，对是否做日志等进行说明。扩展访问控制列表的例子如下：

```
access-list 101 deny tcp 192.168.30.0 0.0.0.255 192.168.31.111 0.0.0.255 eq www log
```

表示该规则序号为101,禁止192.168.30.0网段内的主机建立与192.168.31.111主机的WWW端口(80)的连接,并对违反此规则的事件做日志。

2. 在路由器上实现NAT功能

网络地址转换NAT(Network Address Translation)的最初应用主要是把私有地址转换为公有地址,以节省互联网上的IPv4地址空间。通过NAT转换后,内部的私有IP主机系统的地址被转换为公有IP,来使用互联网上的全局路由网络。在地址转换的同时,NAT可以保护内部网络。由于内部使用私有IP地址,对互联网来说是非路由网络地址范围,使得公网无法发起对内部私有IP地址主机的连接,但内部私有IP地址主机可以发起与公网的连接,NAT技术对内部网络起到了隐藏保护作用,从而降低了内部网络受到攻击的风险。

根据实际使用的环境与需求,NAT主要有以下三种类型的应用。

(1) 一对一的静态NAT转换

内部私有地址与给定的公有地址进行一对一的映射转换,并且为双向的转换。这种类型的NAT可应用于防火墙DMZ接口或路由器内部的服务器区中对外提供服务的服务器,如Web、DNS、FTP等。例如,Web服务器内部私有IP地址为192.168.2.100,一对一的静态NAT转换为200.1.1.3。

(2) 多对多的动态NAT地址池转换

在企业网络接入互联网时,一般都可以从ISP获取一个连续的公网IP地址段,如200.1.1.0/29,其中可用的主机公网IP地址为200.1.1.1～200.1.1.6。其中,一个为ISP的网关地址(如200.1.1.1),一个配置给企业路由器或防火墙的外网接口的公网IP地址(如200.1.1.2),其余公网IP可用于地址池200.1.1.3～200.1.1.6,用于对内部的多台主机进行多对多的转换。例如,192.168.1.2～192.168.1.10对应转换为地址池200.1.1.3～200.1.1.6中的公网地址。由于企业网内部的主机数量往往多于地址池,不能保证所有内部主机同时访问公网,所以动态NAT地址池转换多与后面的PAT结合,实现对地址池的充分利用。

(3) 基于端口多路复用的NAT转换

这种方式下,多个私有地址对应一个公网IP地址。多个内部私有地址变换为统一的外部公有地址,为了同时通信,对公有地址动态配置不同的端口号,与多个内部私有地址进行映射。这在公有IP数少时使用,也是在路由器上应用最多的NAT类型,称为PAT。例如,192.168.1.1～192.168.1.254对应200.1.1.1:1024～65535的PAT转换。

路由器上NAT转换配置的步骤如下:

① (全局模式)access-list 访问号 1 {permit|deny} 反掩码号 [established]。

② access-list 访问号 {permit|deny} IP/TCP协议 源网络 目的网络。

③ ip nat pool cey1 218.62.88.87 218.62.88.89 netmask 255.255.255.192。

④ 在内部网接口上 ip nat inside。

⑤ 在外部网接口上 ip nat outside。

⑥ access-list 1 permit 192.168.1.0 0.0.0.255。

⑦ ip nat inside source list 1 pool cey1 overload。

13.3 方案设计

方案设计如表 13-1 所示。

表 13-1 方案设计

任务名称	设置企业网中路由器安全
任务分解	1. 路由器配置访问控制列表,实现简单包过滤 (1) 画图并连线 (2) 配置各主机和设备的 IP 地址 (3) 路由器访问控制列表 ACL 配置 2. 企业网络中路由设备 NAT 策略部署 (1) 利用 Packet Tracer 画图并连线 (2) 配置各主机和设备的 IP 地址 (3) 路由器包过滤及 NAT 配置 (4) 进行访问控制效果检测
能力目标	1. 能对路由器进行访问控制列表 ACL 配置 2. 能对路由器进行包过滤及 NAT 配置
知识目标	1. 熟悉访问控制列表的种类及使用格式 2. 了解 NAT 的原理及作用 3. 掌握 NAT 的分类 4. 熟悉路由器上配置 NAT 的步骤
素质目标	1. 树立较强的安全意识 2. 掌握网络安全行业的基本情况 3. 培养吃苦耐劳、实事求是、一丝不苟的工作态度 4. 培养分析能力和应变能力 5. 培养创新能力

13.4 任务实施

13.4.1 任务 1:路由器配置访问控制列表,实现简单包过滤

1. 任务目标

在路由器中配置访问控制列表,实现简单的包过滤技术,可以利用 Packet Tracer 软件完成。模拟企业与外部网络的连接拓扑图如图 13-1 所示,计算机 A 和计算机 B 所在网络代表企业网络,计算机 A 和计算机 B 所在网络以外的网络及主机代表外部网络。要求计算机 B 可以访问外部网络,只有 A 不能访问外部网络,外部网络中只有 B 可以 Telnet 远程登录到 C 和 D 主机及其网络。

IP 地址信息如表 13-2 所示。

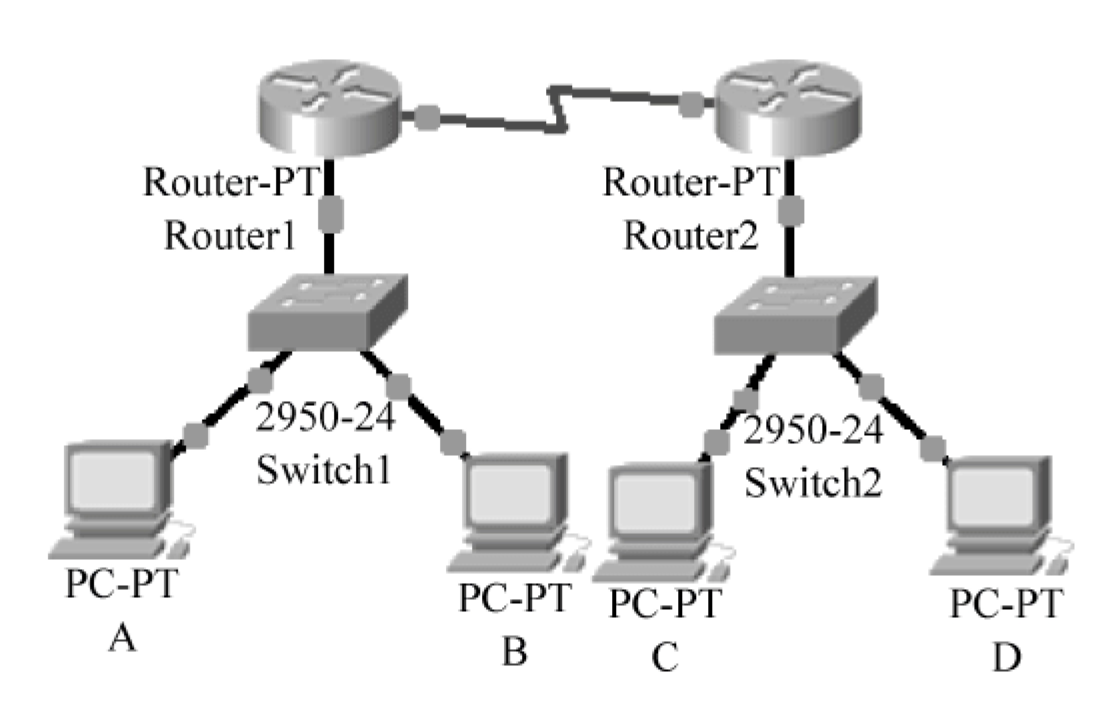


图 13-1　网络拓扑图(1)

表 13-2　IP 地址信息表(1)

R1-S2/0-IP	10.1.1.1	R2-S2/0-IP	10.1.1.2
R1-f0/0-IP	172.16.1.254	R2-f0/0-IP	192.168.1.254
A-IP	172.16.1.1	C-IP	192.168.1.1
B-IP	172.16.1.2	D-IP	192.168.1.2
A 和 B 网关	172.16.1.254	C 和 D 网关	192.168.1.254

2. 工作任务

(1) 画图并连线;

(2) 配置各主机和设备的 IP 地址;

(3) 路由器访问控制列表 ACL 配置。

3. 工作环境

软件工具:Packet Tracer。

4. 实施过程

(1) 画图并连线

在思科模拟工具软件 Packet Tracer 中按照网络拓扑图画图并连线。选择路由器时,注意要有 Serial 口。

(2) 配置各主机和设备的 IP 地址

对照 IP 信息表,对各主机完成 IP 地址、子网掩码和网关地址的配置,并对路由器完成端口 IP 的配置。可以用命令行方式完成,也可以在图形界面中设置。

(3) 路由器访问控制列表 ACL 配置

R1 配置命令如下:

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 172.16.1.254 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 10.1.1.1 255.0.0.0
```

```
Router(config-if)#clock rate 64000
Router(config-if)# no shutdown
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 172.16.1.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#access-list 88 deny host 172.16.1.1
Router(config)#access-list 88 permit any
Router(config)# interface FastEthernet0/0
Router(config-if)#ip access-group 88 in
Router(config-if)#exit
Router(config)#exit
Router#write
```

R2 配置命令如下：

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 10.1.1.2 255.0.0.0
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#access-list 101 permit tcp host 172.16.1.2 192.168.1.0 0.0.0.255 eq telnet
Router(config)# interface FastEthernet0/0
Router(config-if)#ip access-group 101 out
Router(config-if)#exit
Router(config)#exit
Router#write
```

13.4.2 任务 2：企业网络中路由设备 NAT 策略部署

1. 任务目标

利用 PacketTracer 软件模拟企业与外部网络的连接，拓扑图如图 13-2 所示。计算机 A、计算机 B 和计算机 C 所在网络代表企业网络，计算机 D 所在的网络代表外部网络。在路由器中配置 NAT 和 ACL，使得 A、B、C 主机通过 NAT 后可以访问外网主机 D，并可利用内网地址 192.168.2.100 访问 Web 服务器；外网主机也可以访问 Web 服务器，但需要通过公网地址 200.1.1.3 去访问。配置 ACL 功能，仅不允许主机 B 和主机 D 进行 ICMP 通信。

IP 地址信息如表 13-3 所示。

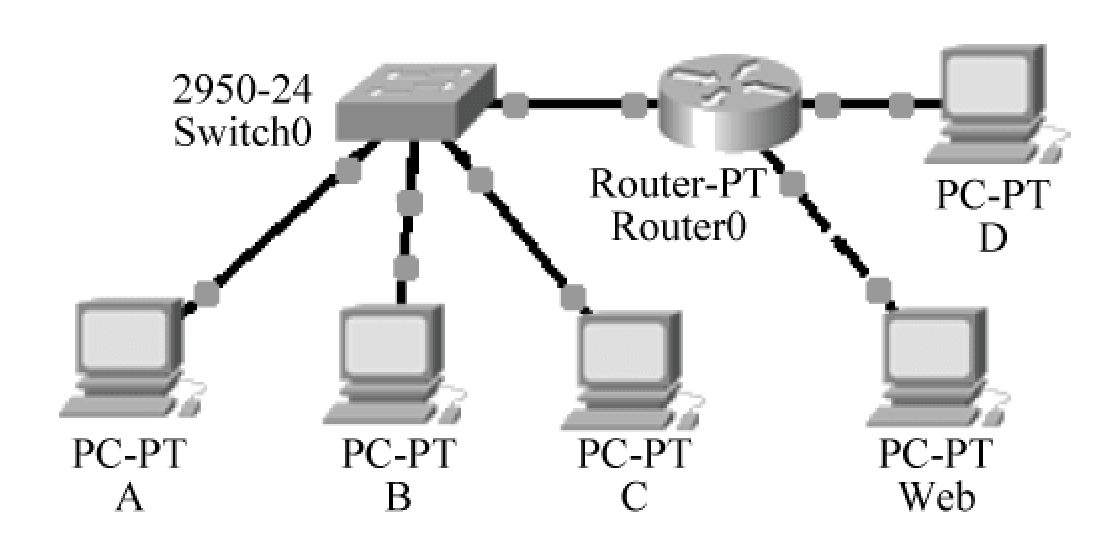


图 13-2　网络拓扑图(2)

表 13-3　IP 地址信息表(2)

R0-f0/0-IP	192.168.1.1	R0-f1/0-IP	200.1.1.1
A-IP	192.168.1.2	R0-f6/0-IP	192.168.2.1
B-IP	192.168.1.3	Web 服务器-内网 IP	192.168.1.4
C-IP	192.168.1.4	Web 服务器-外网 IP	200.1.1.3
D-IP	200.1.1.2	Web 服务器的网关	192.168.1.1
A、B、C 的网关	192.168.1.1		

2. 工作任务

(1) 利用 Packet Tracer 画图并连线;

(2) 配置各主机和设备的 IP 地址;

(3) 路由器包过滤及 NAT 配置;

(4) 进行访问控制效果检测。

3. 工作环境

软件工具:Packet Tracer。

4. 实施过程

(1) 利用 Packet Tracer 画图并连线

在思科模拟工具软件 Packet Tracer 中按照网络拓扑图画图并连线。

(2) 配置各主机和设备的 IP 地址

对照 IP 信息表,对各主机完成 IP 地址、子网掩码和网关地址的配置,并对路由器完成端口 IP 的配置。可以用命令行方式完成,也可以在图形界面中设置。

(3) 路由器包过滤及 NAT 配置

R0 配置命令如下:

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip access-group 110 in
                                    //符合 110 列表规则的数据包进入 f0/0 时进行相应的访问控制
Router(config-if)#ip nat inside     //接口 f0/0 为 NAT 地址转换的内部
Router(config-if)#exit
Router(config)#interface FastEthernet6/0
```

```
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip nat inside            //接口 f6/0 为 NAT 地址转换的内部
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 200.1.1.1 255.255.255.0
Router(config-if)#ip nat outside           //接口 f1/0 为 NAT 地址转换的外部
Router(config-if)#ip nat inside source list 10 interface FastEthernet1/0 overload
  //对于列表 10 中定义的源地址进行动态超载 NAT(PAT)转换,并都转换成 f1/0 接口的公网地址
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip nat inside source static 192.168.2.100 200.1.1.3
  //定义 Web 服务器的静态转换地址
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
  //定义 NAT 的源地址
Router(config)#access-list 10 permit 192.168.2.0 0.0.0.255
  //定义 NAT 的源地址
Router(config)#access-list 110 deny icmp host 192.168.1.3 host 200.1.1.2
  //禁止主机 B 与主机 D 进行 ICMP 通信
Router(config)#access-list 110 permit ip any any
  //允许主机 B 以外的主机进行 IP 通信
```

（4）进行访问控制效果检测

① 对 NAT 转换的检查与测试。在主机 A 上 ping 主机 D,正常为连通状态;但在主机 D 上 ping 主机 A 是不通的,因为 NAT 屏蔽了内部主机。此时,证明 NAT 动态转换设置是正确的。

② 对 Web 服务器访问的检查与测试。分别在主机 A 和主机 D 上访问 Web 服务,A 访问 Web 服务器的内网 IP 地址是192.168.1.4,主机 D 访问 Web 服务器外网 NAT 静态转换后的 IP 地址为 200.1.1.3。如果能分别 ping 通,说明对 Web 服务器的一对一静态 NAT 转换配置正确。

③ 对包过滤 ACL 功能的检查与测试。分别在主机 A 和主机 B 上 ping 主机 D,检查连通性。配置正确后,B 应该无法与 D 进行基于 ICMP 协议的通信,而主机 A 和路由器接口的 IP 都可以跟 D 进行基于 ICMP 协议的通信。

13.5 常见问题解答

1. 访问控制列表的配置原则是什么?

答:访问控制列表(Access Control List,ACL)是路由器接口的指令列表,用来控制从端口进出的数据包。ACL 的默认执行顺序是自上而下。在配置 ACL 列表时,要遵循最小特权原则、最靠近受控对象原则以及默认丢弃原则。其中,最小特权原则是指只给受控对象完成任务所必需的最小的权限,即被控制的总规则是各个规则的交集,只满足部分条件的是不允许通过规则的。最靠近受控对象原则是对所有的网络层访问权限进行控制,也就是说,在检查规则时,自上而下在 ACL 中一条条检测,只要发现符合条件就立刻转发,而不继续检测下面的 ACL 语句。默认丢弃原则是指在路由交换设备中,默认最后一条 ACL 语句是 deny any any,即丢弃所有不符合条件的数据包。

2. 如果 Packet Tracer 软件中的路由器以太网接口不够,该如何操作?

答:如果路由器以太网接口不够,可以先移除 2 个串口后再添加 2 个以太网接口,具体的操作是:单击图 13-3 中电源开关,关闭路由器电源;然后选择图中左侧模块中的"PT-ROUTER-NM-1CFE";再拖动图中右下角的图标到路由器图中的空插槽处;添加完成后,单击电源开关开启路由器电源;最后,选择"命令行"选项卡,进行路由器的命令行配置。

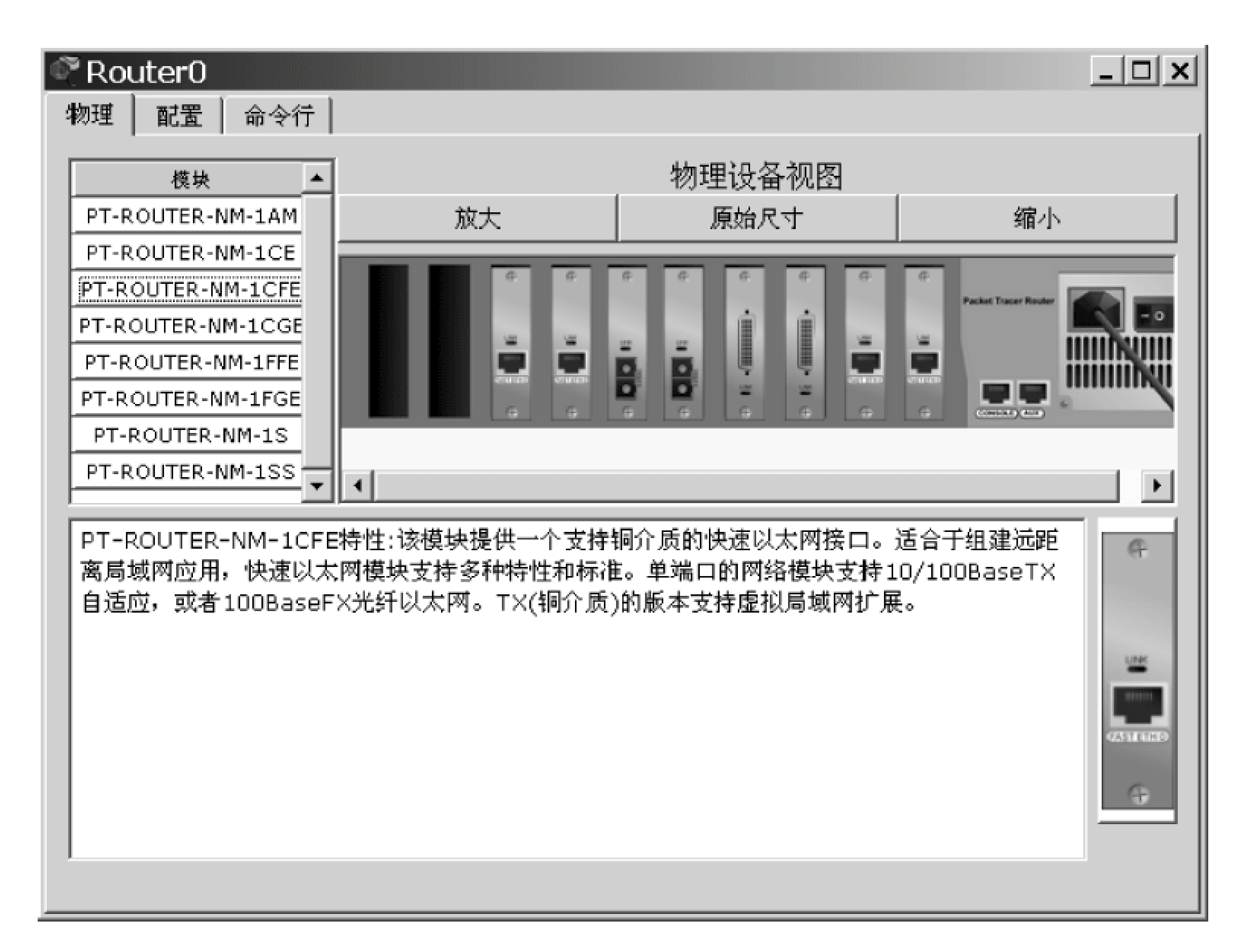


图 13-3　Packet Tracer 软件设备的物理配置

13.6　过 关 练 习

一、选择题

1. 路由器命令"Router(config)# access-list 1 permit 192.168.1.1"的含义是(　　)。
   A. 不允许源地址为 192.168.1.1 的分组通过,如果分组不匹配,则结束
   B. 允许源地址为 192.168.1.1 的分组通过,如果分组不匹配,则检查下一条语句
   C. 不允许目标地址为 192.168.1.1 的分组通过,如果分组不匹配,则结束
   D. 允许目标地址为 192.168.1.1 的分组通过,如果分组不匹配,则检查下一条语句

2. 将 ACL 应用到路由器接口的命令是(　　)。
   A. Router(config-if)# ip access-group 10 out
   B. Router(config-if)# apply accss-list 10 out
   C. Router(config-if)# fixup access-list 10 out
   D. Router(config-if)# route access-group 10 out

3. 以下 ACL 语句中,含义为"允许 172.168.0.0/24 网段所有 PC 访问 10.1.0.10 中的 FTP 服务"的是(　　)。
   A. access-list 101 deny tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp

B. access-list 101 permit tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp

C. access-list 101 deny tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp

D. access-list 101 permit tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp

二、简答题

网络地址转换 NAT 的实现方式有哪三种?

工作任务十四

防火墙的配置与应用

14.1 用户需求与分析

在互联网中,防火墙是一种非常有效的网络安全模型,通过它可以隔离风险区域与安全区域之间的连接,同时不妨碍人们对风险区域的访问。防火墙是不同网络间信息的唯一出口,根据企业网的安装策略控制、允许、拒绝、监测出入网络间的信息流,提供安全防范保护功能。通过对防火墙的配置与应用可以达到以下目的:一是限制他人进入内部网络,过滤不安全服务和非法用户;二是防止入侵者接近防御设施;三是限制用户访问特殊站点;四是为监视互联网安全提供方便。

14.2 预 备 知 识

14.2.1 防火墙的功能

传统意义的防火墙用于控制实际的火灾,使火灾被限制在建筑物的某部分,不会蔓延到其他区域。网络安全中的防火墙是在两个网络之间或主机与网络之间执行访问控制策略的一个或一组系统,包括硬件和软件,目的是保护网络免受恶意行为的侵害,并阻止其非法行为。它是将内部网和公共网分隔的特殊网络互联设备或系统。防火墙的内部区域是指内部网络或者内部网络的一部分,是可信任的区域,应受到防火墙的保护。外部区域是指 Internet 或者外部的网络,是不被信任的区域。它能够完成网络用户访问控制、认证服务、数据过滤,限制内部用户访问某些站点等功能。它遵循允许或拒绝业务往来的网络通信安全机制,提供可控的过滤网络通信,只允许授权的通信。防火墙作为一个安全网络的边界点,在不同的网络区域之间进行流量的访问控制。

网络防火墙的工作任务是设置一个检查站,监视、过滤和检查所有流经的协议数据,并对其执行相应的安全策略,如阻止协议数据通过或禁止非法访问,能有效地过滤攻击流量。另外,防火墙通过对网络的访问行为进行记录,即日志记录,同时提供审计功能,完成对网络使用情况的数据、统计与监视功能。防火墙通过 NAT 等技术完成对内部网络信息,如关键主机的 IP 及开启的服务等信息的隐藏与保护,使内部网络不暴露于外网。提供企业网络服务的防火墙能控制和管理网络访问,保护网络和系统资源,对数据流量进行深度检测,还可以验证身份,记录和报告事件。防火墙通过设置 DMZ 接口,发布企业的部分资源与信息服务,如对外提供的 Web、FTP 或 E-mail 等服务。DMZ 称为非军事化区,对于防火墙的 DMZ 口所连接的部分,一般称为服务器群或服务器区,防火墙也可以进行测量的检查与控制,只

允许对特定服务端口的访问进入。如开放的 Web 服务仅当对内部服务访问的目的端口为 80 时才被允许。

14.2.2 防火墙的工作原理

防火墙是网络上的一种过滤器,让安全的信息流通过,不安全的信息全部过滤掉。防火墙采用的技术和标准五花八门、多种多样,但工作方式都一样,即分析出、入防火墙的数据包,决定放行还是阻止通过。所有的防火墙都具有 IP 地址数据包过滤功能,只需要检查 IP 数据包头部特征信息,如根据其 IP 源地址和目标地址,可做出放行还是丢弃的动作。包过滤是在 IP 层实现的,根据包的源 IP 地址、目的 IP 地址、源端口、目的端口及包传递方向等报头信息来判断是否允许包通过。包过滤防火墙的应用非常广泛,因为 CPU 用于处理包过滤的时间几乎可以忽略不计,并且这种防护措施对用户透明,合法用户在进出网络时,根本感受不到它的存在,使用起来很方便。因此这样的系统具有很好的传输性能,并容易扩展。缺点是这种防火墙不太安全,包过滤防火墙对应用层性能无法解析,如果攻击者把自己主机的 IP 地址设置成一个合法主机的 IP 地址,就可以轻易通过包过滤器防火墙。代理服务型防火墙在应用层上实现防火墙功能,弥补了包过滤防火墙的不足。它能提供部分与传输有关的状态,提供与应用有关的状态,解析部分传输的信息,还能处理和管理信息。

在技术实现上,防火墙经历了第一代的包过滤技术阶段,最典型的是设计在路由器上的访问控制列表(ACL)功能完成包过滤防火墙的功能;1989 年推出的电路层防火墙和应用层防火墙被认为是第二代和第三代防火墙的初步结构;1992 年开发出的基于动态包过滤技术的防火墙被称为第四代防火墙;1998 年 NAI 公司推出的自适应代理技术可以称为第五代防火墙。

较早的防火墙是在路由器上实现的,随着互联网应用的普及,出现了建立在通用操作系统上的防火墙,目前已经发展为具有安全的专用操作系统的防火墙,并多以独立的硬件设备形式在网络中部署,但仍然是软件和硬件的结合,只是较多的功能通过硬件实现,如在对数据进行 VPN 传输的保护中,性能较好的防火墙采用专用的硬件完成加密处理,如 DES 加密等。

14.2.3 防火墙的分类

市场上各种防火墙产品繁多,划分的标准各式各样,主要的分类有以下几种。

(1) 按操作对象不同分为主机防火墙和网络防火墙。主机防火墙的优点是位置优势、低成本;缺点是难以部署和维护,缺乏透明度,功能局限性,比如天网防火墙、诺顿防火墙。网络防火墙的优点是功能强大、性能高、透明度强;缺点是成本高、内部攻击保护性差,例如锐捷防火墙、蓝盾防火墙、天融信网络卫士。

(2) 按实现方式不同分为软件防火墙和硬件防火墙。软件防火墙用于应用层控制和检测,优点是功能丰富,缺点是性能低、有自身安全性问题。例如,微软的 ISA 防火墙、checkpoint 防火墙。硬件防火墙的优点是性能高、自身安全性高、易于维护,缺点是缺乏高级功能。例如,锐捷防火墙、思科防火墙、蓝盾防火墙和天融信网络卫士。

(3) 按技术实现层次分为网络层防火墙和应用层防火墙。网络层防火墙通过对流经的协议数据包的头部信息,如源地址、目的地址、协议号、源端口和目的端口等信息进行规定策略的控制。应用层防火墙可以对协议数据流进行全面的检查与分析,确定需执行策略的控制。

(4) 按过滤和检测方式分为包过滤防火墙、状态防火墙、应用网关防火墙、地址转换防火墙、透明防火墙和混合防火墙。无状态包过滤防火墙的技术优点是处理速度快,缺点是无法阻止应用层攻击,部署复杂,维护量大。它是互联网边界的第一层防线,隐式拒绝,显示允许。例如,使用 ACL 过滤的路由器。有状态包过滤防火墙技术与无状态包过滤防火墙执行相似操作,优点是保持对连接状态的跟踪,能监视更高级的信息,例如特定应用层协议检测;缺点是不能阻止应用层攻击,状态表导致系统开销增大。它作为主要的防御措施,需要更加严格的控制。支持应用层检测的状态防火墙采用动态协议检测,能检测应用层报头中的信息。应用网关防火墙采用应用网关防火墙技术,通常称为代理防火墙,支持身份验证,能监控和过滤应用层信息。支持的应用有限,可能需要部署客户端软件,作为主要的防护措施需要更严格的身份及会话验证。连接网关防火墙执行传统的应用网关防火墙检测方式。直通代理防火墙是简化的应用网关防火墙,对于初始连接请求进行身份验证,具有更好的性能。地址转换防火墙解决了公有 IP 地址匮乏的问题,隐藏了内部网络结构,引入了延时,破坏了 IP 的端到端模型。透明防火墙充当网桥的角色,易于部署,即插即用,零配置,无须更改编制结构和路由拓扑,隐蔽性高,无 IP,无连接可达到。

(5) 按部署位置不同分为边界防火墙、个人防火墙和混合防火墙。

(6) 按性能不同分为百兆级防火墙和千兆级防火墙。

14.2.4　PIX 防火墙配置

PIX 防火墙提供非特权模式、特权模式、配置模式和监视模式等四种管理访问模式。在配置模式下,命令 nameif 用于配置防火墙接口的名字,并指定安全级别。默认情况下,端口 Ethernet0 被命名为外部接口(Outside),安全级别为 0;端口 Ethernet1 被命名为内部接口(Inside),安全级别为 100。用户可配置的安全级别取值范围为 1～99,数字越大,安全级别越高。在配置模式下,命令 interface 可用于配置防火墙接口的数据传输速率。选项 auto 表明接口采用自动协商方式,100full 表示采用 100Mb/s 全双工通信。在配置模式下,命令 ip address 可用于配置防火墙接口的 IP 地址。

在配置模式下,命令 nat 用于指定要进行转换的内部地址,命令 global 用于指定外部 IP 地址范围(即地址池)。命令 nat 总是与命令 global 一起使用,因为命令 nat 可以指定一台主机或一段 IP 地址范围的主机访问外网。访问外网时,需要利用命令 global 所指定的地址池进行对外访问。

命令 nat 的语法格式是

```
nat (if_name) nat_id local_ip [netmask]
```

其中,if_name 是内网接口名字,例如 inside;nat_id 是全局地址池标识,使它与其相应的 global 命令相匹配;local_ip 是内网被分配的 IP 地址;netmask 是内网 IP 地址的子网掩码。

例如,启用 NAT,设定内网的所有主机均可访问外网的配置命令是

```
firewall(config)#nat (inside) 1 0.0.0.0 0.0.0.0
```

也可以写成

```
firewall(config)# nat (inside) 1 0 0
```

命令 global 的语法格式是

```
global (if_name) nat_id ip_address-ip_address [netmask global_mask]
```

其中，if_ name 是外网接口的名字，例如 outside；nat_id 是全局地址池标识；ip_address-ip_address 是 NAT 转换后的单个 IP 地址或某段 IP 地址范围；netmask global_mask 是全局 IP 地址的子网掩码。

例如，当内网的所有主机要访问外网时，防火墙将送往 Internet 的 IP 数据包的源地址统一映射为 202.10.10.1 的配置语句是

```
firewall(config)#global (outside) 1 202.10.10.1
```

配置外网地址池为 202.10.20.1～202.10.20.10。当内网主机访问外网时，将地址统一映射到该 IP 地址池的配置语句是

```
firewall(config)#global (outside) 1 202.10.20.1-202.10.20.10
```

在配置模式下，命令 route 用于设置指向内网和外网的静态路由，其语法格式是

```
route(if_name)0 0 gateway_ip [metric]
```

其中，if_name 是接口名字，例如 inside、outside；gateway_ip 是网关路由器的 IP 地址；metric 是到 gateway_ip 的跳数，其默认值为 1。

在配置模式下，命令 static 将内部地址翻译成一个指定的全局地址，其命令格式是

```
static (internal_ip_name,external_if_name) outside_ip_address inside_ip_address
```

例如，当地址为 192.168.0.1 的内网主机访问外网时，地址静态转换为 202.10.10.1。使用 static 命令创建外部 IP 地址 202.10.10.1 和内部 IP 地址 192.168.0.1 之间静态映射的配置命令是

```
firewall(config)#static (inside,outside) 192.168.0.1 202.10.10.1
```

在配置模式下，命令 conduit 用于允许数据流从具有较低安全级别的接口流向具有较高安全级别的接口，其命令格式是

```
conduit permit|deny global_ip port [-port] protocol foreign_ip [netmask]
```

例如，使用 202.10.10.1 这一 IP 地址对外网提供 Web 服务，并允许所有的外网用户访问的配置命令为

```
conduit permit tcp host 202.10.10.1 eq www any
```

允许 ICMP 消息以任意方向通过防火墙的配置命令为

```
conduit permit icmp any any
```

在配置模式下，命令 fixup 用于启用、禁止、改变一个服务或协议通过防火墙，其命令格式是

```
fixup protocol <protocol> [port]
```

例如，启用 HTTP 服务，并指定该 HTTP 使用的端口号为 8080 的配置命令为

```
firewall(config)#fixup protocol http 8080
```

禁用端口号为21的FTP的配置命令为

```
firewall(config)# no fixup protocol ftp 21
```

14.2.5 防火墙的选用

目前，在国内防火墙产品市场中，国内产品和国外产品各占半壁江山。国外品牌的优势主要是技术和知名度比国内产品高。国内品牌则对国内用户需求了解更加透彻，价格上也具有优势。国外防火墙厂商主要有思科(Cisco PIX)、CheckPoint、NetScreen等，特点是自身开发能力强，产品线比较齐全，有比较完善的销售渠道和技术支持体系。它们的主要客户是电信、金融等高端用户群。国内防火墙一线厂商主要有东软、天融信、启明星辰、联想、方正、安氏领信、华为等，产品应用领域较广，从高端到低端都有覆盖，网络应用从百兆位到千兆位，产品针对性较强。

防火墙的主要性能指标如下：

(1) 吞吐量。在不丢包情况下能够达到的最大速率。

(2) 时延。入口输入帧最后一个比特到达出口处，输出帧第一个比特输出所用的时间间隔，体现了防火墙处理数据的速度。

(3) 丢包率。在连续负载情况下，应转发却未转发帧的百分比。丢包率对防火墙稳定性和可靠性有较大影响。

(4) 并发连接数。穿越防火墙的主机之间或主机与防火墙之间能同时建立的最大连接数，反映了防火墙对来自客户端TCP连接请求的响应能力。

(5) 最大并发连接数建立速率。单位时间内建立的最大连接数，体现了防火墙单位时间内建立和维持TCP连接的能力。

目前，市场有6种基本类型的防火墙，分别是嵌入式防火墙、基于企业软件的防火墙、基于企业硬件的防火墙、SOHO软件防火墙、SOHO硬件防火墙和特殊防火墙。在防火墙产品选购中，用户通常考虑的要点如表14-1所示。

表14-1　防火墙产品选购要点

自身的安全性	主要体现在自身设计和管理两个方面
系统的稳定性	通过权威评测机构测试、实际调查、自己试用、厂商的研制历史、厂商实力等方法判断
是否高效	一般防火墙加载上百条规则，性能下降不应超过5%
是否可靠	提高可靠性的措施一般是提高本身部件的强健性、增大设计阈值和增加冗余部件，这要求有较高的生产标准和设计冗余度
功能是否灵活	要求有一系列不同级别，满足不同用户的各类安全控制需求的控制策略
配置是否方便	支持透明通信，在安装时不需要对原网络配置做任何改动
管理是否简便	在充分考虑安全需要的前提下，必须提供安全、灵活的管理方式和方法，体现为管理途径、管理工具和管理权限
是否可以抵御拒绝服务攻击	需详细考察这一功能的真实性和有效性
是否可以针对用户身份过滤	常用一次性口令验证机制，来确认登录用户身份
是否可扩展、可升级	如果不支持软件升级，用户需要更换硬件，更换期间网络不设防，同时花费较大

14.3 方案设计

方案设计如表 14-2 所示。

表 14-2 方案设计

任务名称	防火墙的配置与应用
任务分解	1. 防火墙的典型安装与部署 (1) 防火墙的连接与登录配置 (2) 防火墙透明模式(网桥模式)的典型安装与部署 (3) 防火墙 NAT 模式(路由模式)的典型安装与部署 2. 使用防火墙实现策略管理 (1) 架设实验环境 (2) 实验分析 (3) 检查各点网络状况 (4) 设置端口映射,实现访问的互通 (5) 为 LAN 内 PC 设置对外访问策略,实现访问的互通 3. 使用防火墙进行流量控制 (1) 启动带宽管理 (2) 配置网络流量策略 (3) 添加网络流量应用规则 (4) 配置 P2P 功能 (5) 添加固定流量规则
能力目标	1. 掌握防火墙的基本连线方法 2. 能使用管理端口登录到防火墙上进行配置 3. 能实现防火墙透明模式的典型安装和配置 4. 能实现防火墙 NAT 模式的典型安装和配置 5. 能设置防火墙端口映射,实现外网访问内网 Web 服务器 6. 能设置防火墙策略,实现局域网内计算机访问外网 7. 能启动防火墙带宽管理 8. 能配置防火墙网络流量策略 9. 能配置防火墙 P2P 功能 10. 能添加防火墙网络流量应用规则 11. 能添加防火墙固定流量规则
知识目标	1. 掌握防火墙的功能 2. 了解防火墙的工作原理 3. 熟悉防火墙的分类 4. 了解 PIX 防火墙的网络接口地址初始化配置 5. 了解 PIX 防火墙的网络地址转换(NAT)配置
素质目标	1. 掌握网络安全行业的基本情况 2. 树立较强的安全意识 3. 培养吃苦耐劳、实事求是、一丝不苟的工作态度 4. 培养分析能力和应变能力 5. 具有可持续发展能力

14.4 任务实施

为了完成本工作任务，又细分为以下4个子任务。

14.4.1　任务1：防火墙的典型安装与部署

1. 任务目标

掌握防火墙的基本连线方法，了解防火墙的基本设置、管理模式和操作规范。掌握防火墙在透明模式下工作时，对内、外网口的配置及添加桥接的规则，最后通过从内网ping通路由来验证桥接正确部署。

2. 工作任务

(1) 防火墙的连接与登录配置；

(2) 防火墙透明模式(网桥模式)的典型安装与部署；

(3) 防火墙NAT模式(路由模式)的典型安装与部署。

3. 工作环境

(1) 三台预装Windows Server 2003/XP的主机。

(2) 一台防火墙设备、一台二层交换机、一台三层交换机、一台路由器。

4. 实施过程

(1) 防火墙的连接与登录配置

① 单线接第1组蓝盾防火墙的第一口，默认IP为192.168.11.1，在IE输入https://192.168.11.1:81；第2组蓝盾防火墙第一口，默认IP为192.168.12.1，在IE输入https://192.168.12.1:81；第3组蓝盾防火墙第一口，默认IP为192.168.13.1，在IE输入https://192.168.13.1:81；第4组蓝盾防火墙第一口，默认IP为192.168.14.1，在IE输入https://192.168.14.1:81；第5组蓝盾防火墙第一口，默认IP为192.168.15.1，在IE输入https://192.168.15.1:81；第6组蓝盾防火墙第一口，默认IP为192.168.16.1，在IE输入https://192.168.16.1:81；第7组蓝盾防火墙第一口，默认IP为192.168.17.1，在IE输入https://192.168.17.1:81；第8组蓝盾防火墙第一口，默认IP为192.168.18.1，在IE输入https://192.168.18. 1:81。统一用户密码为admin/888888。

② 配置网口IP，单击“网络配置”→“网口设置”，如图14-1所示。

③ 如配置外网口，选择相应网口的“配置WAN”，如图14-2所示。

④ 单击“保存”按钮，然后进入之前的网口配置界面，配置内网口，如图14-3所示。

⑤ 配置重定向策略，单击“防火墙”→“NAT策略”，配置后如图14-4所示。

⑥ 配置防火墙的管理设置。因为默认只有第一口能够访问，需做策略，让2、3口能够访问管理，单击“系统”→“管理设置”，如图14-5所示。

(2) 防火墙透明模式(网桥模式)的典型安装与部署

在透明模式(桥接模式)下，防火墙相当于一个网桥，通过将两个网口桥接起来，即将交换机和路由器直接连接起来，从而无须改动原有网络结构，将防火墙透明地加入网络。对于连接内网的LAN2口，其IP地址要设成和内网在同一个网段。透明模式适用于内网、外网

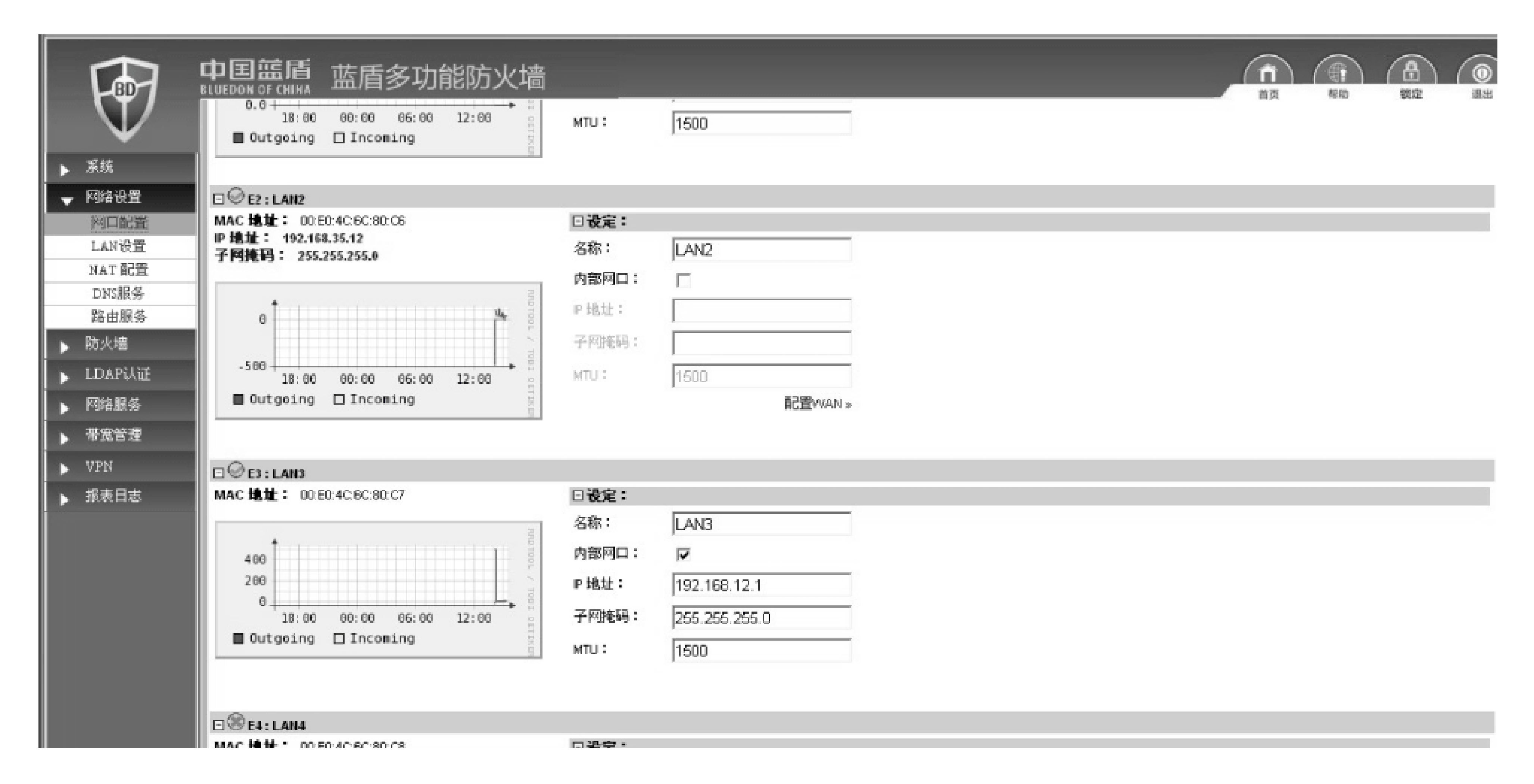


图 14-1 “网口设置”窗口



图 14-2 “NAT 连接”窗口

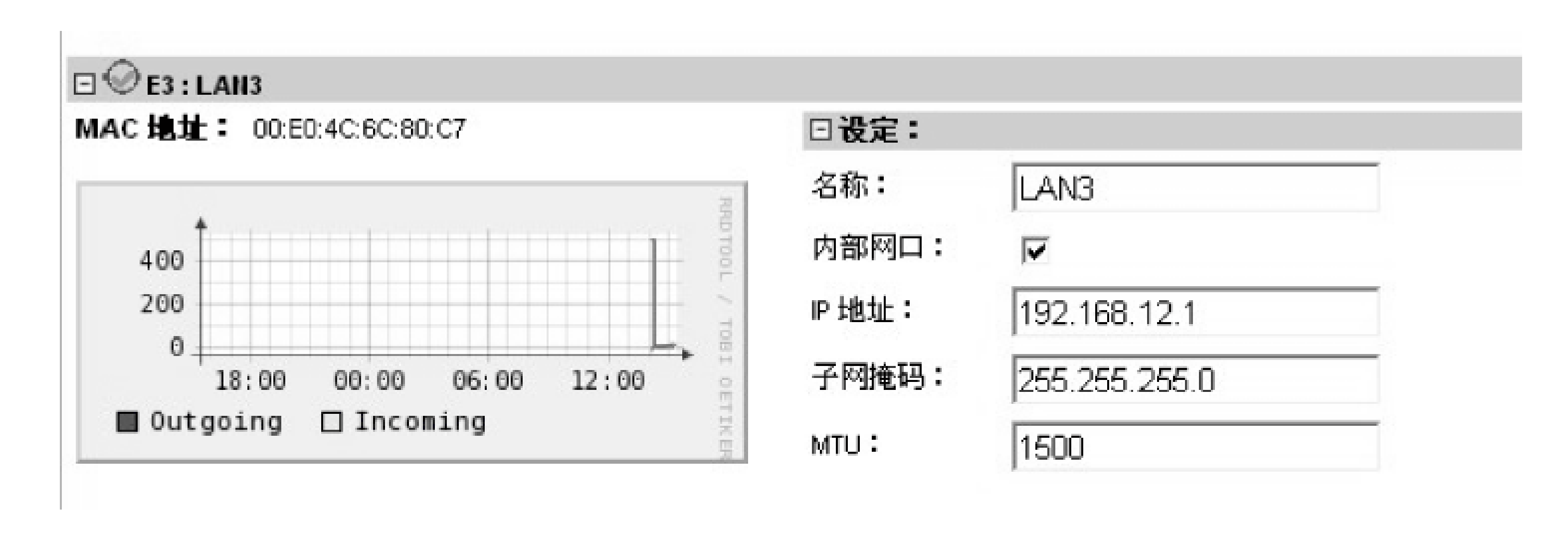


图 14-3 配置内网口

和 DMZ 区域等同在一个网段的情况，网络拓扑如图 14-6 所示。

① 将防火墙按照图 14-6 所示接入当前网络。由路由器引入的外线接 WAN 口，由交换机引出的内部网线接 LAN 口。



图 14-4　“NAT 策略”窗口



图 14-5　“管理界面访问设定”窗口

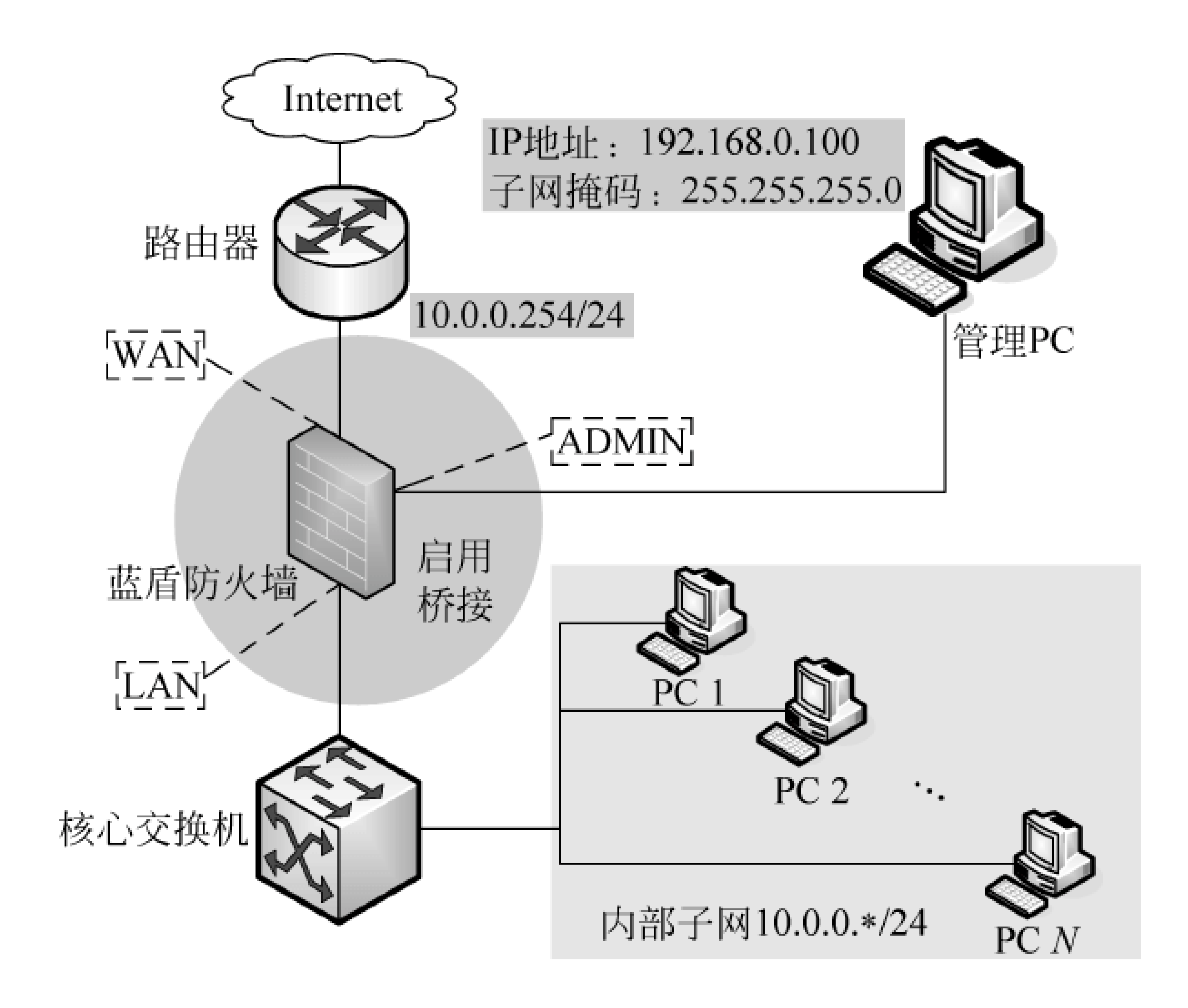


图 14-6　网络拓扑图(1)

② 检验加入后的网络状况，从内部网络中的任一台 PC 无法再 ping 通路由器的对内网口 IP 地址 10.0.0.254。

③ 通过管理 PC 登录防火墙系统，单击“系统”→“系统信息”→“设备状态”，查看网络接口信息，可以看到当前的线路连接。WAN 口上由于没有配置 IP，无流量进、出，故仍显示 ，如图 14-7 所示。

网络接口信息

网口	类型	IP 地址	stat	RX bytes	TX bytes
LAN1	管理	192.168.0.101		4747337	5236154
LAN2	内部	192.168.1.1		2273531	630
LAN3	内部	172.16.0.1		0	0
LAN4	外部				

图 14-7 网络接口信息(1)

由于桥接要求网口不能是内网口，并且在该网口上没有配置外线连接，因此需要对 LAN 口进行一些设置。

④ 单击“网络设置”→“网口配置”→“网口设置”，进入桥接设定界面，如图 14-8 所示。

网口设置

选择分页大小 20 1 /1 3 条记录 刷新

序号	网口	名称	类型	MAC 地址	IP 地址	子网掩码	MTU	速率	监听	启动	☐
1	LAN1	LAN	管理	00:0C:29:38:EF:CD	192.168.1.1	255.255.255.0	1500	auto			☑
2	LAN2	DMZ	内部	00:0C:29:38:EF:D7	192.168.0.1	255.255.255.0	1500	auto			☐
3	LAN3	WAN	外部	00:0C:29:38:EF:E1			1500	auto			☐

启动 编辑

图 14-8 网口设置(1)

⑤ 单击“编辑”按钮后，将 LAN 口的“类型”设置为“外部网口”，然后单击“保存”按钮。单击“启动”按钮，将 LAN 口设置为外网口，如图 14-9 所示。



图 14-9 LAN 设置

⑥ 单击“网络设置”→“网口配置”→“桥接设定”，进入桥接设定界面，启用桥接，如图 14-10 所示。

⑦ 定义一条桥接规则，如图 14-11 所示。

参数定义：

- 名称：为桥定义一个名称。
- MAC 地址：为桥定义一个 MAC 地址。
- IP 地址：为桥定义一个 IP 地址。
- 子网掩码：IP 地址的子网掩码。
- 左框：可用于添加到桥的网口，必须是外部网口。



图 14-10 “桥接设定”窗口

连接：
名称： br0
MAC 地址：
IP 地址： 10.0.0.1
子网掩码： 255.255.255.0
Select DEV
>>>
<<<
LAN2
LAN4
启用：
添加

图 14-11 定义桥接规则

• 右框(Select DEV)：已经添加到桥内的网口。
• 启用：勾选，则单击“添加”时同时启用。

⑧ 添加一条桥接规则，如图 14-12 所示。

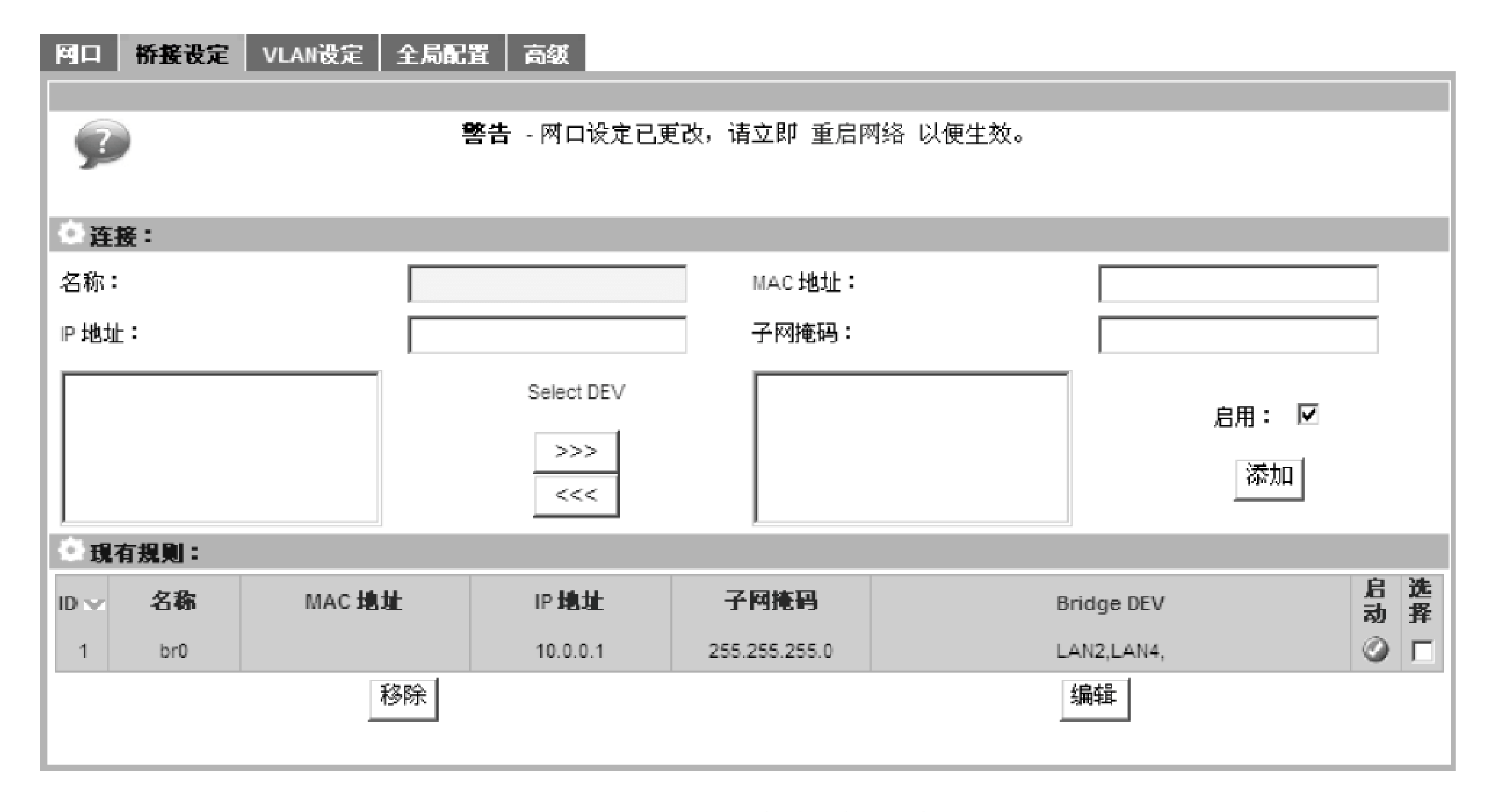


图 14-12 添加桥接规则

⑨ 添加成功后，在“现有规则”中会出现一条之前定义的规则，同时系统检测到网口设定已更改，要求重启网络。重启网络。

⑩ 测试桥接，检查 LAN 内主机是否能 ping 通路由地址。从内网任一台主机发起 ping 到路由器，可以连通，则防火墙桥接模式(透明模式)部署成功。

注意：防火墙的初始规则是默认阻挡所有流量，在本实验中，为了方便实验，所有设备预设是全部允许，在接下来的 NAT 部署模式中也是预设全部允许通过，除此之外，在其他实验中都是默认全部拒绝。

(3) 防火墙 NAT 模式(路由模式)的典型安装与部署

① 将防火墙按照图 14-13 所示接入当前网络，由路由器引入的外线接 WAN 口，由核心交换机引出的内部网线接 LAN 口，由 DMZ 区域的交换机引出的网线接 DMZ 口。

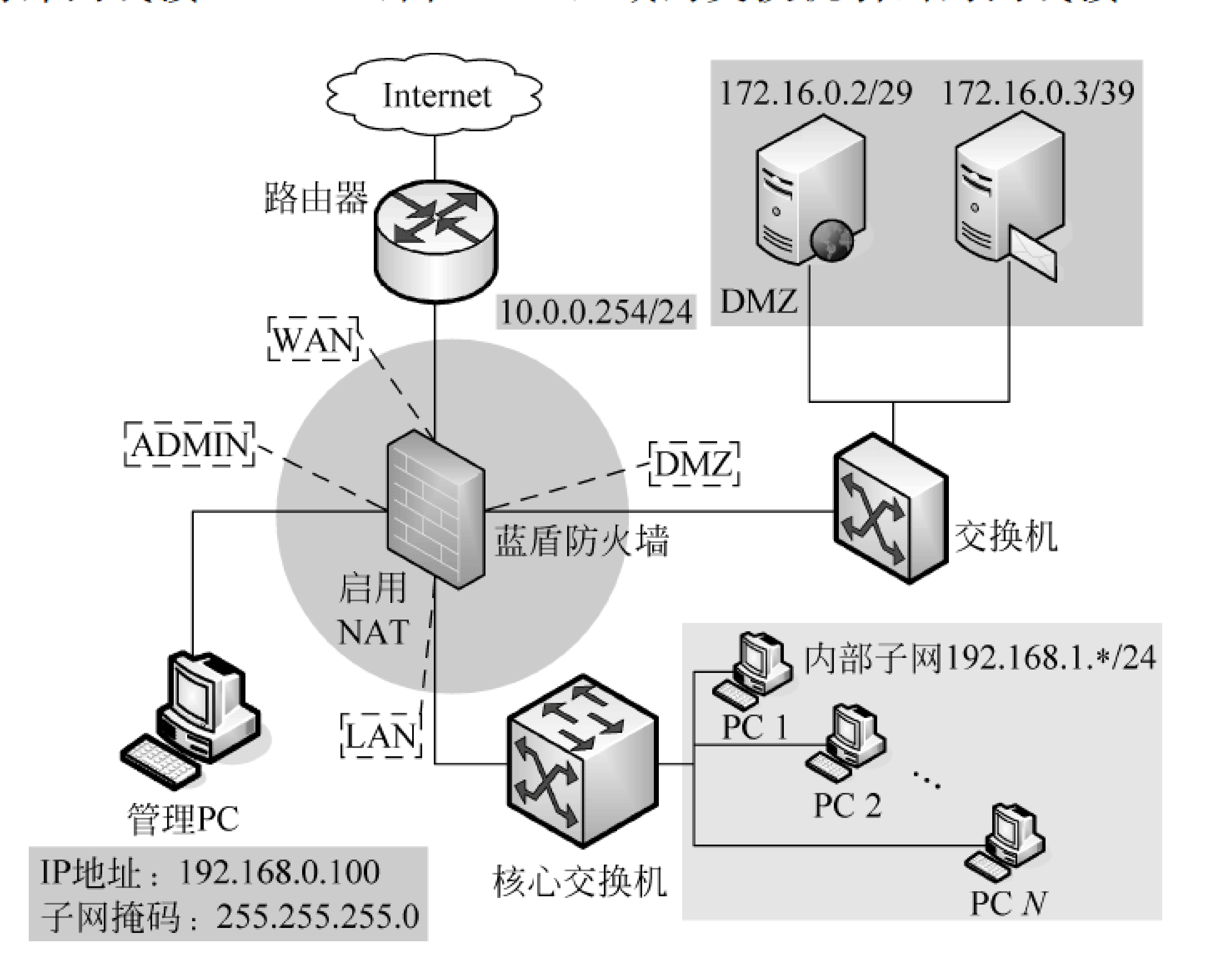


图 14-13 网络拓扑图(2)

② 检验加入防火墙后的网络状况，从内部网络中的任一台 PC 无法再 ping 通路由器的对内网口 IP：10.0.0.254。

③ 通过管理 PC 登录防火墙系统，然后单击“系统”→“系统信息”→“设备状态”，查看网络接口信息，可以看到当前的线路连接。WAN 口上由于没有配置 IP，无流量进、出，故仍显示 ，如图 14-14 所示。

网络接口信息

网口	类型	IP 地址	stat	RX bytes	TX bytes
LAN1	管理	192.168.1.1		40858342	52367513
LAN2	内部	192.168.0.1		0	210
LAN3	外部			0	0

图 14-14 网络接口信息(2)

④ 进入网口配置界面，然后单击“网络设置”→“网口配置”→“网口”查看接口情况，如图 14-15 所示。

网口设置

选择分页大小 20　1 /1　3 条记录　刷新

序号	网口	名称	类型	MAC 地址	IP 地址	子网掩码	MTU	速率	监听	启动	
1	LAN1	LAN	管理	00:0C:29:38:EF:CD	192.168.1.1	255.255.255.0	1500	auto			
2	LAN2	DMZ	内部	00:0C:29:38:EF:D7	192.168.0.1	255.255.255.0	1500	auto			
3	LAN3	WAN	外部	00:0C:29:38:EF:E1			1500	auto			

启动　编辑

图 14-15 网口设置(2)

⑤ 修改内网主机 IP 配置，将内网中的主机 IP 设置为与防火墙设备 LAN 口同一网段的地址，并将网关指向 LAN 口地址。

⑥ 修改 DMZ 区域服务器 IP 配置，使网关指向 DMZ 口。

⑦ 测试 LAN 和 DMZ 区域是否与对应网口连通。在完成修改的 PC 上 ping LAN 口地址，在完成修改的 PC 上 ping DMZ 口地址，能 ping 通，说明 LAN 和 DMZ 内部主机已与防火墙的网口互通了。

⑧ 配置防火墙的 WAN 口，然后单击“网络设置”→“NAT 配置”→“NAT 连接”进行 NAT 配置，如图 14-16 所示。

连接：
WAN-LINK　选择　删除　名称：　WAN-LINK

图 14-16　连接设置

参数定义：

- 左框：选择一个连接。
- 名称：为连接定义一个名称。

⑨ 全局设定如图 14-17 所示。

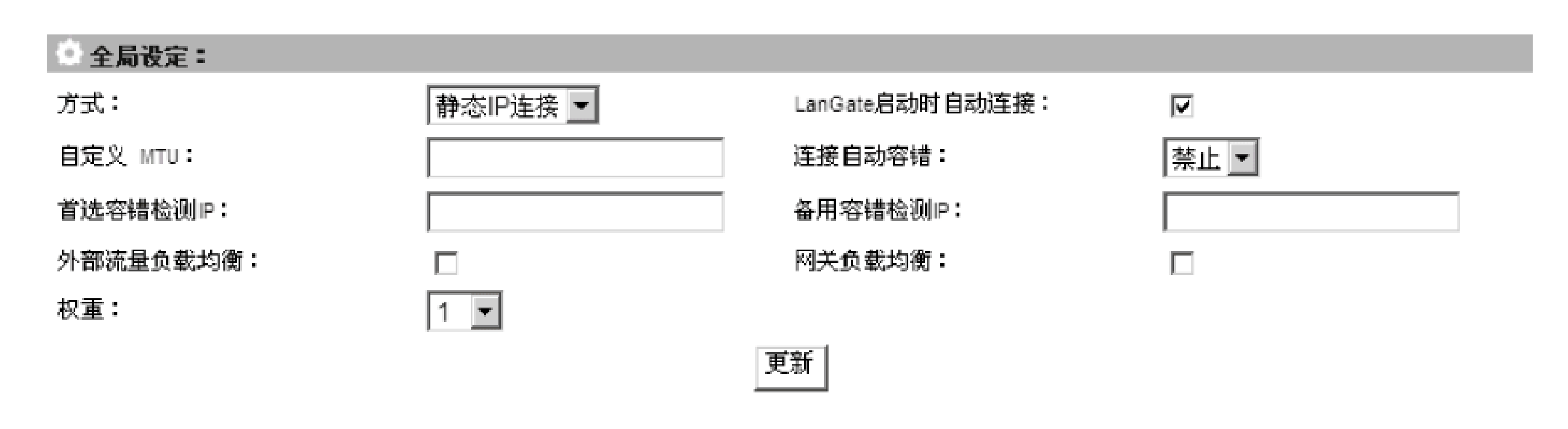


图 14-17　全局设定

参数定义：

- 方式：为连接定义方式。
- LanGate 启动时自动连接：勾选，则在系统启动时会自动采用这个连接。
- 自定义 MTU：设置 MTU 值。
- 连接自动容错：当连接错误时采取动作。
- 首选容错检测 IP：设置首选容错检测 IP。
- 备用容错检测 IP：设置备用容错检测 IP。
- 外部流量负载均衡：是否启用外部流量负载均衡。
- 网关负载均衡：是否启用网关负载均衡。
- 权重：设置权重值。

⑩ 连接方式有静态 IP 连接、动态 IP 连接、PPPoE 和 PPTP 四种，自动容错方式包括禁止、重启和 TEST。选择不同的连接方式，然后单击“更新”，会出现相应的设定项（以静态连接为例），如图 14-18 所示。

参数定义：

- 网口：选择当前可用的外部网口。



图 14-18　静态 IP 连接设定

- 默认网关：指向上网网关。
- IP 地址：设置可上网的 IP 地址。
- 子网掩码：设置子网掩码。
- 首选 DNS 服务器：设置首选 DNS 服务器。
- 备用 DNS 服务器：设置备用 DNS 服务器。

⑪ 在“全局配置”中选择“静态连接配置”，接着进行静态 IP 连接的设定。

⑫ 单击“系统”→“系统信息”，可以查看到连接信息。若设置正确，可以看到网络已经连接。由于防火墙设备能够根据网口信息自动建立路由表，因此此时内部子网可以连接到防火墙上层的路由器，如图 14-19 所示。

⊟路由

目标地	网关	子网掩码	标记	度量	网口
172.16.0.0	0.0.0.0	255.255.255.248	U	0	LAN3
10.0.0.0	0.0.0.0	255.255.255.0	U	0	LAN4
192.168.0.0	0.0.0.0	255.255.255.0	U	0	LAN1
0.0.0.0	10.0.0.254	0.0.0.0	UG	0	LAN4

图 14-19　连接信息

⑬ 检查内网是否 ping 通外网。从内网任一台主机发起 ping 到路由器，若可以连通，说明防火墙的 NAT 模式部署成功。

14.4.2　任务 2：使用防火墙实现策略管理

1. 任务目标

了解策略管理的意义；熟练掌握配置访问策略的方法，包括服务对象、访问目的、访问源、动作的设置；熟练掌握配置策略映射的方法；掌握配置 LAN 与 WAN 间的互访规则的方法并进行验证。

2. 工作任务

(1) 架设实验环境；

(2) 实验分析；

(3) 检查各点网络状况；

(4) 设置端口映射，实现访问的互通；

(5) 为 LAN 内 PC 设置对外访问策略，实现访问的互通。

3. 工作环境

(1) 三台预装 Windows Server 2003/XP 的主机。

(2) 一台防火墙设备、一台二层交换机、一台三层交换机、一台路由器。

4. 实施过程

(1) 架设实验环境

按照图 14-20 所示完成线路连接。WAN 口接入一台 PC 作为外部主机(开启 22 端口和 21 端口,即 SSH 服务和 FTP 服务),地址为 10.0.0.100/24,网关指向 10.0.0.1;DMZ 口接入一个 Web 服务器提供 Web 服务,地址为 172.16.0.2/29,网关指向 172.16.0.1;LAN 区域接入一个 192.168.1.0/24 的子网,网关指向 192.168.1.1。

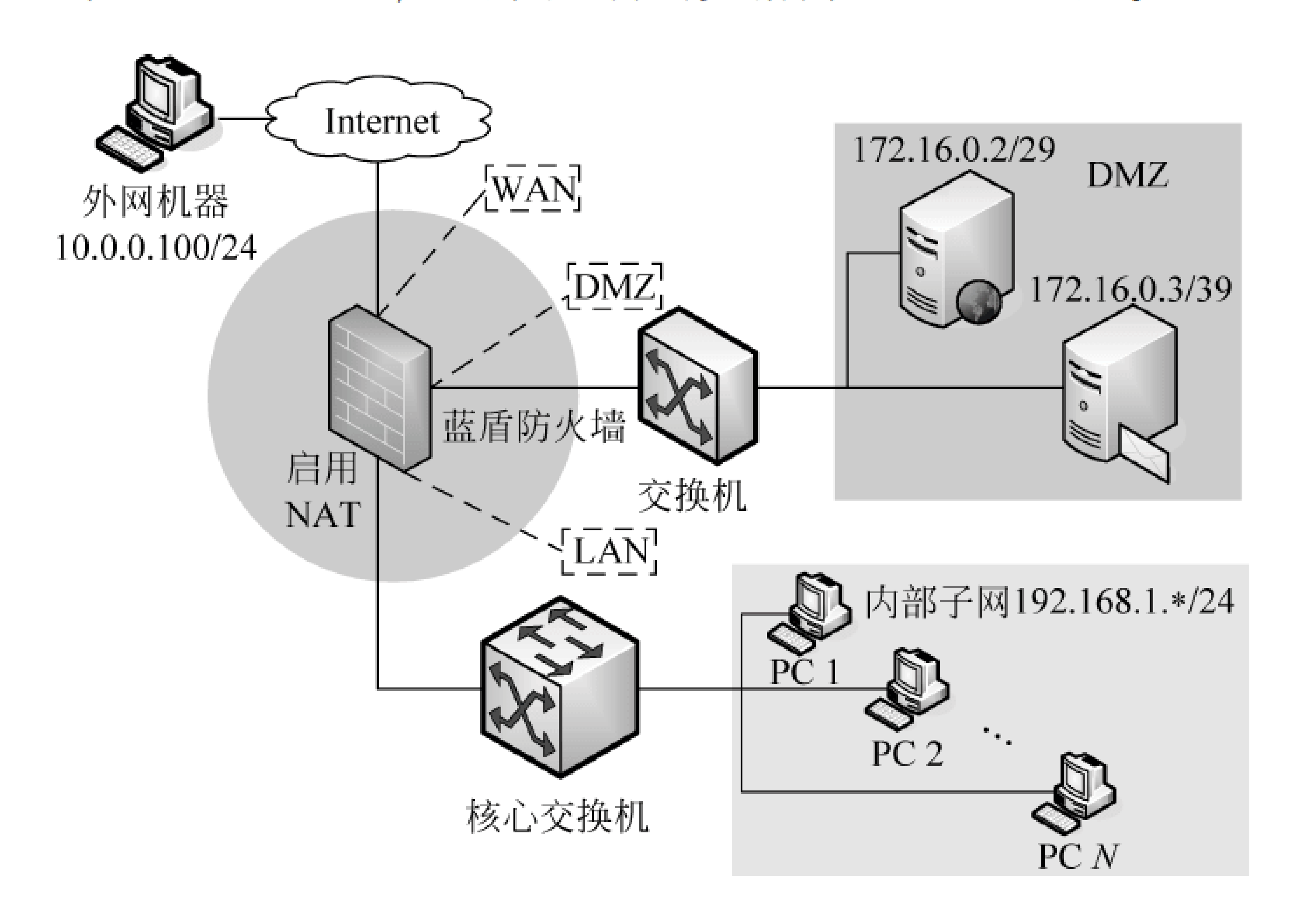


图 14-20 网络拓扑图(3)

(2) 实验分析

默认情况下,连接在防火墙不同网口的网络是不能互相访问的。为了使各个网络间实现互通,需要建立网络间的通信通道。外网访问内网通过端口映射机制实现,内网访问外网通过设置访问规则控制,它们都是通过建立通信规则,并将规则应用到不同网口、网段或 IP 上实现。

(3) 检查各点网络状况

① 外部主机(10.0.0.100/24)可以 ping 通防火墙的 WAN 口地址(10.0.0.1),但是没有办法到达 DMZ 区的 Web 服务器(172.16.0.2)。因为对于 10.0.0.100 来说,Web 服务器的地址是一个其他网络的内网地址。

② Web 服务器(172.16.0.2/29)主机无法 ping 通外网 PC(10.0.0.100),因为防火墙上默认拒绝连出。

③ LAN 区主机(192.168.1.2/24)无法 ping 通外网 PC(10.0.0.100)。

由于当前网络被防火墙隔离了,使得内、外网无法互访,这时通过端口映射的方式,使得外网可以访问内部网络,同时通过策略设置,使内网可以访问外网。

(4) 设置端口映射,实现访问的互通

一个端口映射可以把所有外部对内部的某种请求映射到部署在 DMZ 的网站服务器的任一端口。本实验中 Web 服务器的 IP 为 172.16.0.2/29,要访问到 Web 服务器提供的服务,就要使所有外部 80 端口的访问都指向 172.16.0.2/29 的 80 端口。

① 单击"防火墙"→"NAT 策略"→"DNAT 策略"界面,选择对应的外网连接,如图 14-21 所示。



图 14-21　外部接口设置

② 设置规则参数，填写源端口、目标 IP、目标端口，然后选择“启用”，如图 14-22 所示。

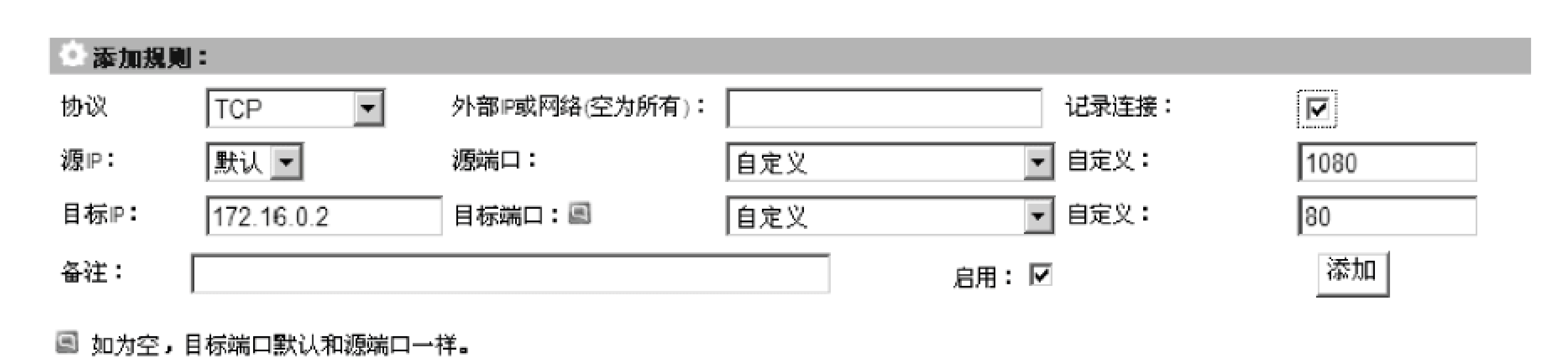


图 14-22　添加规则(1)

参数定义：

- 协议：定义连接使用的协议。
- 外部 IP 或网络(空为所有)：设置允许连接的外部 IP 或网络，留空代表任意值。
- 记录连接：记录使用该端口映射的网络数据。
- 源 IP：访问到防火墙的外部网口或外部别名，为默认选项。
- 源端口：映射到的访问端口，这里指外部连接 Web 服务器时采用的端口。
- 目标 IP：端口映射到的目标 IP，这里指 Web 服务器的 IP 地址。
- 目标端口：端口映射到的目标端口，这里指 Web 服务器将被访问的端口。

在端口选择时，系统预定义了很多公认端口；也可以选择确定端口；还可以选择“自定义”，然后在后面的框中填入具体的端口值。

③ 这里把外网地址 10.0.0.1 的 80 端口映射到 172.16.0.2 的 80 端口，就是说，当访问 10.0.0.1 的 80 端口时，防火墙会把这个地址自动映射为 172.16.0.2 的 80 端口。

④ 查看“现有规则”，如图 14-23 所示。

现有规则：

ID	协议	外部 IP	源 IP	源端口	目标IP	目标端口	记录	启动	选择
				备注					
5	TCP	ALL	默认	HTTP (80)	172.16.0.2	HTTP (80)			

图 14-23　查看“现有规则”(1)

这时，一个外网访问内网的通道被打开。注意，在创建端口映射时要十分谨慎，因为端口映射为外部网络访问内部网络提供了一个通道，如果被黑客使用，可能会访问目标 IP 并通过目标 IP 访问其他主机。

⑤ 验证设置。外部主机(10.0.0.100/24)通过 http://10.0.0.1 可以访问 DMZ 区的 Web 服务器；DMZ 区的 Web 服务器(172.16.0.2/29)主机仍然无法 ping 通外网 PC(10.0.0.100)。

(5) 为 LAN 内 PC 设置对外访问策略，实现访问的互通

① 单击“防火墙”→“LAN”→“WAN 策略”→“规则设置”，设置一个访问策略，如图 14-24 所示。

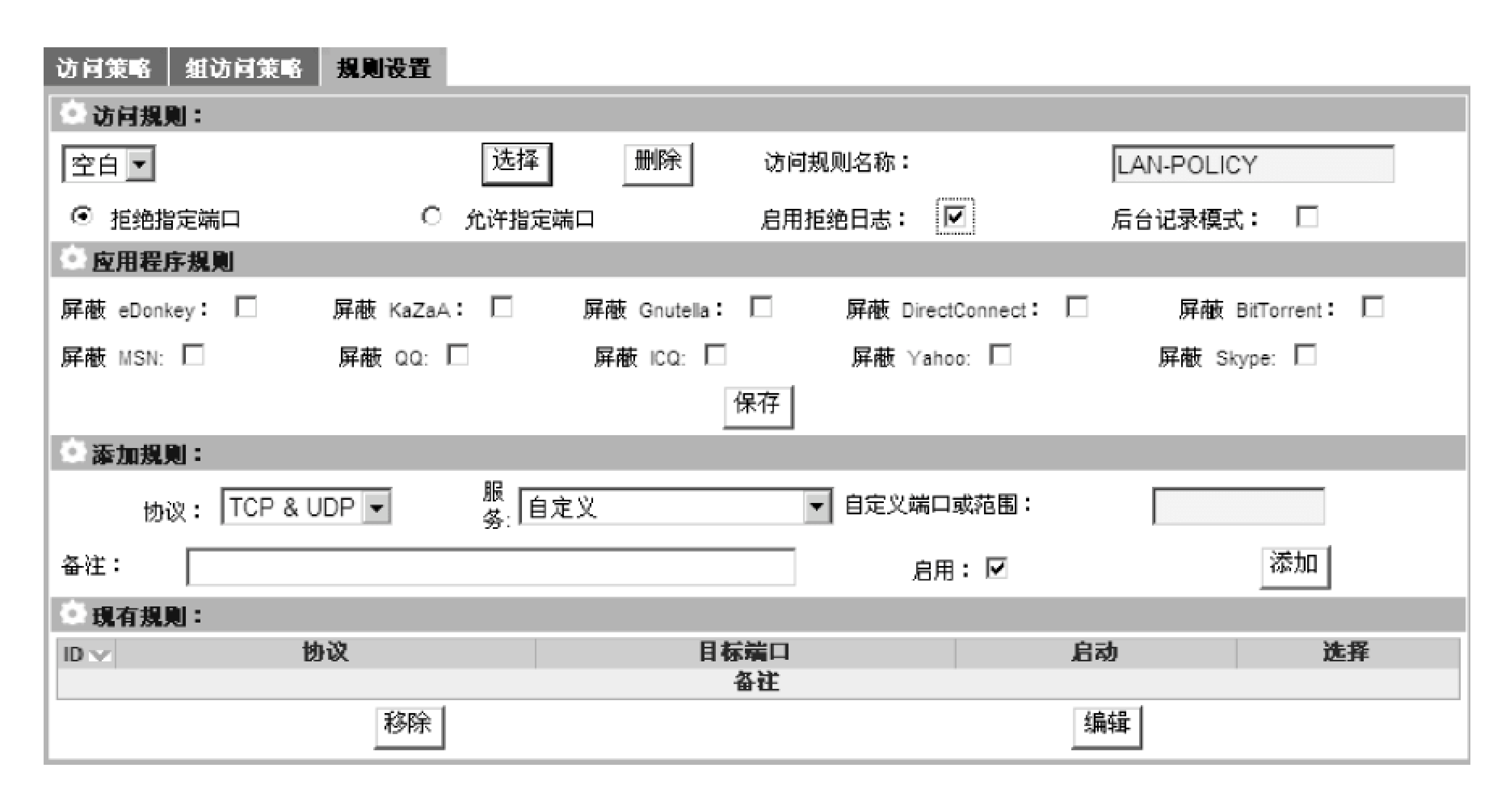


图 14-24　规则设置

参数定义：

- 访问规则名称：定义访问规则的名称。
- 拒绝指定端口：选择该选项，该访问策略中的所有端口将被拒绝访问。
- 允许指定端口：选择该选项，该访问策略中的所有端口将被允许访问。
- 启用拒绝日志：选择该选项，所有违反该访问策略的外部访问将被记录。
- 后台记录模式：选择该选项，所有违反该访问策略的外部访问将被记录，同时不做任何屏蔽。

② 设置完毕后，单击“保存”按钮，就预定义了一条名为“LAN-POLICY”的访问策略。当前策略中定义了“对 FTP 的连接”和“对 123 端口的 UDP 通信”，选择拒绝，应用程序无设置。接下来，将该策略应用到某些 IP 或子网上，如图 14-25 所示。



图 14-25　“LAN-POLICY”的访问策略

③ 单击“防火墙”→“LAN”→“WAN 策略”→“访问策略”，应用该策略，然后填写策略的实施对象，并选择规则，最后单击“添加”按钮，如图 14-26 所示。



图 14-26 添加规则(2)

参数定义：

- 源 IP 或网络：定义访问策略实施的对象。
- 规则：选择要实施的访问策略。

规则中除了有自定义的外，还有全部拒绝和全部允许的选项。

④ 查看“现有规则”，如图 14-27 所示。



图 14-27 查看“现有规则”(2)

⑤ 验证设置。内网 PC(192.168.1.2/24)可以 ping 通外网 PC(10.0.0.100)；内网 PC(192.168.1.2/24)可以访问外网 PC 的 22 端口；内网 PC(192.168.1.2/24)无法访问外网 PC 的 21 端口。

⑥ 查看日志可以看到拒绝记录，要求规则设置时有启用拒绝日志，并且日志设定中有开启防火墙的日志。单击“报表日志”→“系统日志”→“防火墙”，选择种类“启用拒绝日志”，目标 IP 填“10.0.0.100”，最后单击“更新”，可以查看到该记录。

Web 服务器(172.16.0.2/29)无法 ping 通外网 PC。LAN 区域访问外网成功，但是 DMZ 区域依然无法访问外网，说明对外访问策略成功。

14.4.3 任务 3：使用防火墙进行流量控制

1. 任务目标

流量控制是网络安全管理的一项重要应用。通过使用防火墙应能控制网络流量的实现过程。带宽管理包括广义的带宽限制，如针对协议、端口、多个 IP、组用户；也有固定的带宽限制，如针对单个 IP 固定流量等。理解流量控制的意义，掌握配置网络流量策略的方法。

2. 工作任务

(1) 启动带宽管理；

(2) 配置网络流量策略；

(3) 添加网络流量应用规则；

(4) 配置 P2P 功能；

(5) 添加固定流量规则。

3. 工作环境

(1) 一台预装 Windows Server 2003/XP 的主机。

(2) 一台防火墙设备。

4. 实施过程

(1) 启动带宽管理

选择“带宽管理”→“启动控制”→“手动启动”，然后单击“启动”按钮，当前状态显示为“运行”。单击屏幕下方的“保存”按钮，如图 14-28 所示。



图 14-28　带宽管理

(2) 配置网络流量策略

① 如图 14-29 所示，“外部”有端口的上、下行流量设置，用户可根据需求进行设置，完成后单击“保存”按钮。

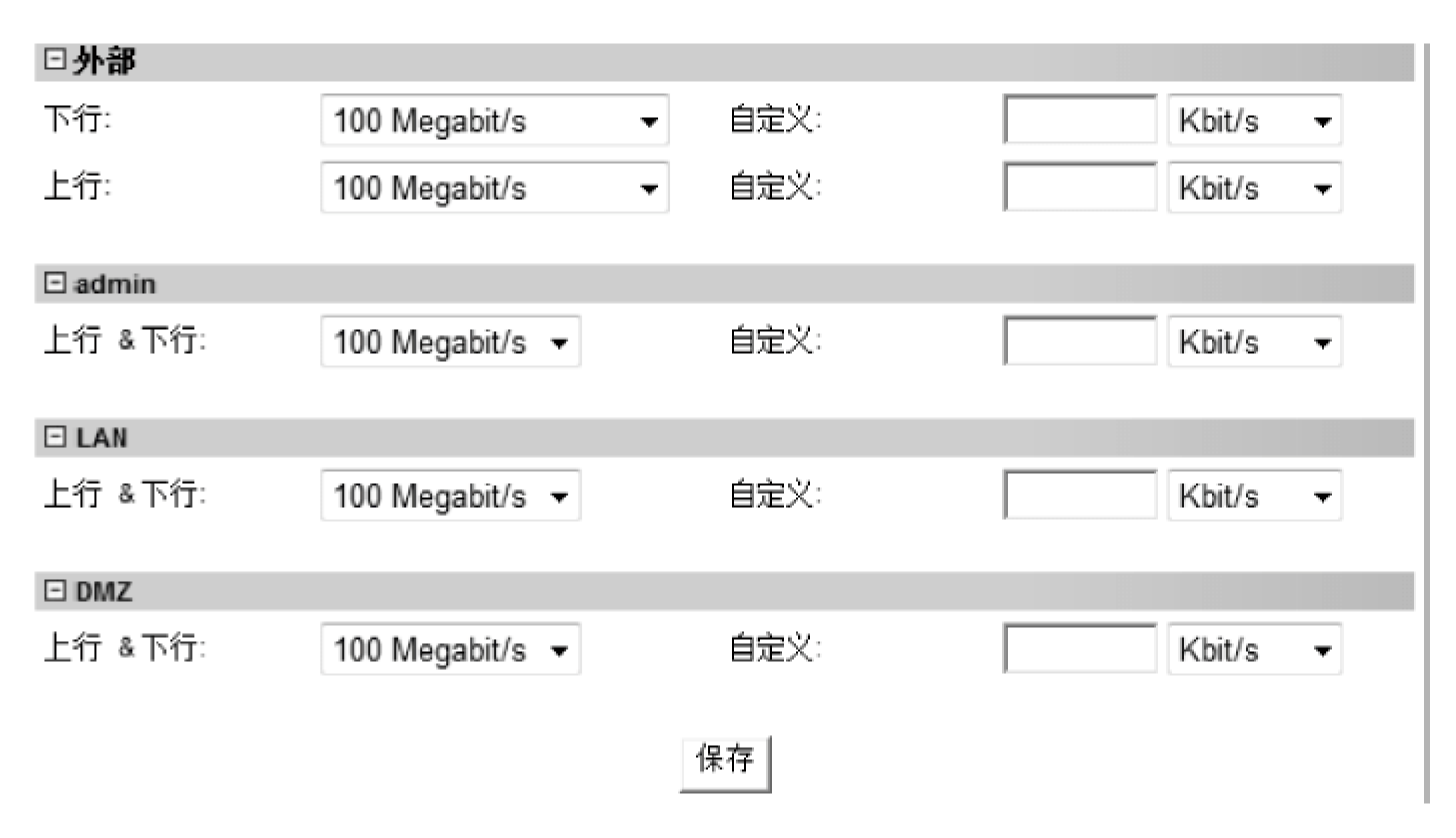


图 14-29　流量设置

② 进入“网络流量策略”界面，单击“添加”按钮，配置流出的 HTTP(80)流量，如图 14-30 所示。

图 14-30　“增加设置”窗口(1)

③“当前流量策略”中将出现新增策略。如需特殊的限制，可在“协议”、“服务”、“流量”和“流向”下拉框中完成相应的选择。如果选择“全局”，则将当前策略应用于内网所有用户，如图 14-31 所示。



图 14-31　新增策略

(3) 添加网络流量应用规则

① 单击“网络流量应用规则”，再单击“添加”按钮，完成配置，如图 14-32 所示。

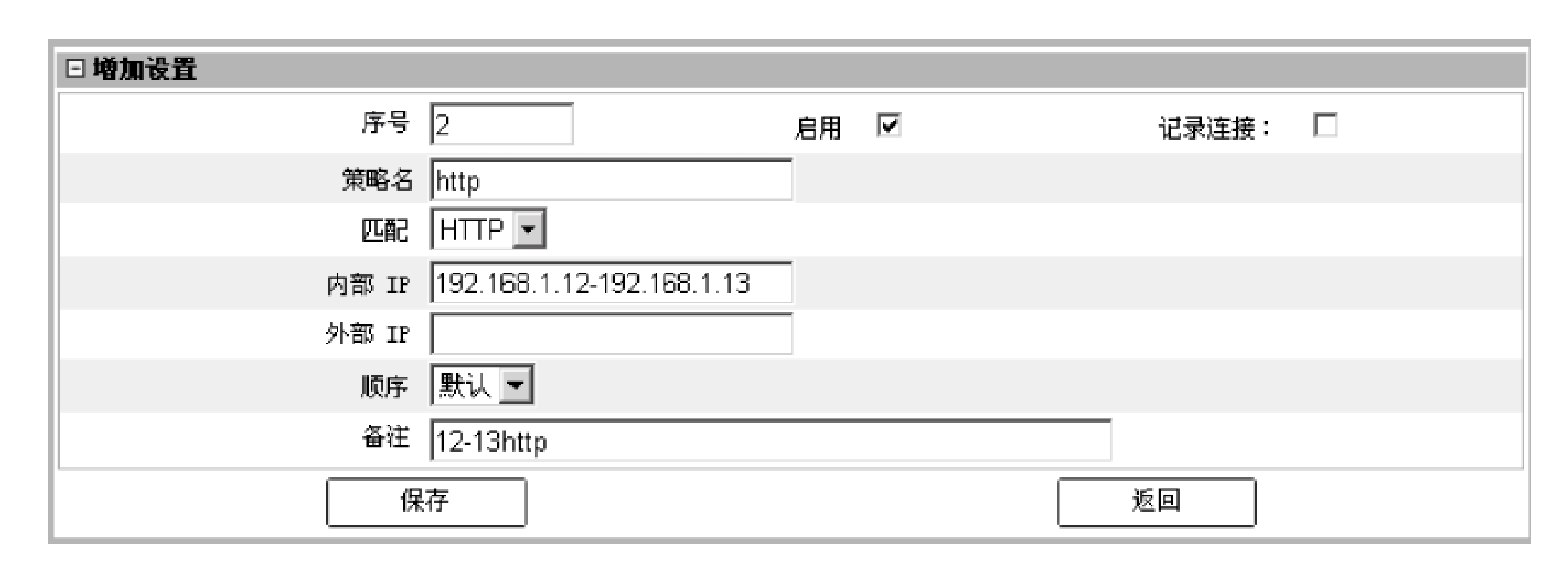


图 14-32　“增加设置”窗口(2)

② 单击“保存”按钮，出现针对 IP 地址 192.168.1.12～192.168.1.13 范围内的共用带宽设置的限制 HTTP 服务的策略，如图 14-33 所示。



图 14-33　“现有网络流量应用规则”窗口

③ 在“内部 IP”中只填入一个 192.168.1.12 用户的 IP，就是只限制一个用户的 HTTP 服务的策略，如图 14-34 所示。

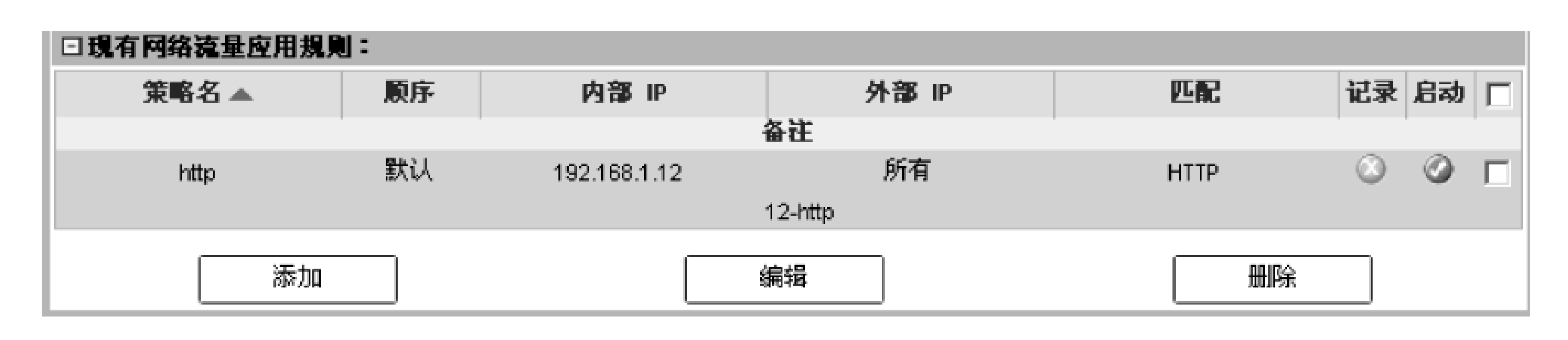


图 14-34　只限制一个用户的策略

(4) 配置 P2P 功能

可以利用 P2P 功能对一些常用的 P2P 软件进行流量种类方面的限制。

① 单击“P2P”进入 P2P 配置窗口，如图 14-35 所示。

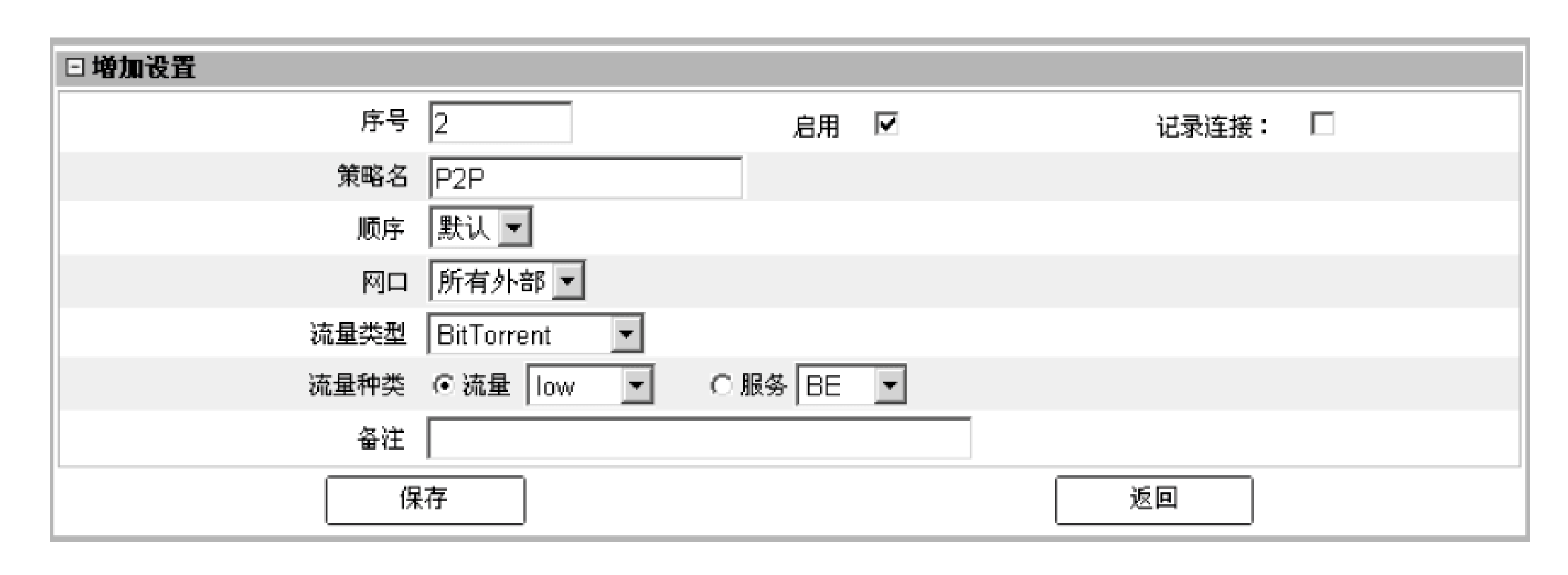


图 14-35　“增加设置”窗口(3)

② 配置完毕后单击“保存”按钮，“当前 P2P 策略”中出现一条针对内部网口的 P2P 限制策略，如图 14-36 所示。



图 14-36　“当前 P2P 策略”窗口

(5) 添加固定流量规则

① 限制流量种类为 low(低级别)，即保证 15%带宽，使用上限为 40%带宽。可以在“网络流量应用规则”中将该策略应用给某个 IP 或是某段 IP，也可应用于全局，如图 14-37 所示。



图 14-37　策略应用

② 添加固定流量规则，可以对从 LAN 口(源)到 WAN 口(目的)出去的 IP 或是某段 IP 进行固定带宽的限制，如图 14-38 所示。

③ 配置完毕后单击“保存”按钮，“现有规则”中将增加一条针对 192.168.1.12～192.168.1.13 用户固定流量带宽的限制规则，如图 14-39 所示。

在没做上述限制的情况下，使用下载工具下载，下载速度会占用整个带宽的最大值。在将上、下行带宽限制为 50KB/s 后，下载速度会限制在 50KB/s 以内。在实际应用中，外部网口、内部网口和上、下行带宽的单位应根据实际情况而定。



图 14-38　添加固定流量规则



图 14-39　配置完成窗口

14.5　常见问题解答

NAT 的分类及作用是什么？

答：网络地址转换（Network Address Translation，NAT）是一个 IETF（Internet Engineering Task Force，Internet 工程任务组）标准，允许一个机构以公网 IP 地址出现在互联网上。换言之，它是一种把内网私有网络地址（IP 地址）翻译成合法公网 IP 地址的技术。NAT 有三种类型：静态 NAT、动态 NAT 和网络地址端口转换（Network Address Port Translation，NAPT）。静态 NAT 是把内部网络中的每台主机都永久映射成外部网络中的某个合法地址。动态 NAT 是在外部网络中定义一系列合法地址，采用动态分配的方法映射到内部网络。网络地址端口转换 NAPT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。动态 NAT 只是转换 IP 地址，它为每个内部 IP 地址分配一个临时的外部 IP 地址，主要应用于拨号。当远程用户连接上之后，动态地址 NAT 就会分配给它一个 IP 地址；当用户断开网络连接时，该 IP 地址会被释放，留待以后使用。NAPT 普遍应用于接入设备中，它将中小型网络隐藏在一个合法的 IP 地址后面。NAPT 与动态 NAT 的不同之处在于，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加一个由 NAT 设备选定的 TCP 端口号。

14.6 过关练习

一、选择题

1. 为了防止局域网外部用户对内部网络的非法访问，可采用的技术是(　　)。

A. 网卡　　B. 网关　　C. 网桥　　D. 防火墙

2. 关于防火墙的功能，以下(　　)描述是错误的。

A. 防火墙能检查进、出内部网的通信量

B. 防火墙能使用应用网关技术在应用层上建立协议过滤和转发功能

C. 防火墙可以使用过滤技术在网络层对数据包进行选择

D. 防火墙能阻止来自网络内部的威胁和攻击

3. 包过滤防火墙通过(　　)来确定数据包是否能通过。

A. 路由表　　B. ARP 表　　C. NAT 表　　D. 过滤规则

4. 包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的检查内容一般不包括(　　)。

A. 源地址　　B. 目的地址　　C. 协议　　D. 有效载荷

二、简答题

防火墙是否可以防范病毒？为什么？

工作任务十五

入侵检测系统IDS的部署与配置

15.1 用户需求与分析

随着网络安全风险不断增大,仅仅使用防火墙作为最主要的安全防范手段来保护网络的安全远远不够,已不能满足人们对网络安全的需求。因为一方面,网络攻击者可能不断地寻找防火墙的漏洞,并且防火墙无法保护防火墙内的网络的安全性;另一方面,防火墙无法提供实时的入侵检测能力。因此,使用入侵检测系统IDS有助于快速发现网络攻击,提高网络安全管理员的安全审计、监视、进攻识别和响应能力。有人将IDS产品比作继杀毒和防火墙产品之后安全领域的第三战场。

15.2 预备知识

15.2.1 入侵检测的功能

入侵检测系统IDS(Intrusion Detection Systems)最早在1980年4月由美国空军在名为《计算机安全威胁监控与监视》的技术报告中提出。它是一种实时的网络入侵检测和响应系统,能够实时监控网络传输;依照一定的安全策略,对被保护的网络流量进行检测,或对系统的运行状况进行监视,自动检测可疑行为;分析来自网络外部和内部的入侵信号,尽可能发现各种攻击企图、攻击行为或攻击结果;在发现有入侵行为或者将要有入侵行为时发出告警,实时对攻击做出响应,并提供补救措施,以保证网络系统资源的机密性、完整性和可用性,最大限度地为网络系统提供安全保障。

常见的入侵检测系统的功能如下:

(1) 网络流量管理。大多数入侵检测系统IDS允许记录、报告和禁止几乎所有形式的网络访问,还可以用它监视某一台主机上通过的所有网络流量。当定义了策略和规则后,在设备上可以捕获到HTTP、FTP、SMTP、Telnet和任何其他流量。这种策略和规则有助于追查网络连接等相关信息。

(2) 系统扫描。入侵检测系统IDS扫描当前网络的活动,监视和记录网络的流量,根据定义好的规则来过滤各种流量,提供实时警报。

(3) 追踪。入侵检测系统IDS不仅能记录安全事件,还可以确定安全事件发生的位置。通过追踪来源,可以更多地了解攻击者。入侵检测系统IDS记录下的日志不仅可以记录攻击过程,同时有助于确定解决方案。

15.2.2　入侵检测的工作原理

本质上，入侵检测系统 IDS 是一个典型的嗅探设备，它在网络上被动地、无声息地收集需要的报文，像公路上的摄像头一样，对攻击者的入侵行为进行监测，对网络安全起保护作用。入侵检测系统 IDS 的运行方式有两种，一种是在目标主机上运行，以监测本身的通信信息；另一种是在一台单独的机器上运行，以监测所有网络设备的通信信息，如 Hub、路由器等。当有某个事件与一个已知攻击的特征相匹配时，多数 IDS 都会报警。

入侵检测系统 IDS 处理网络上数据信息的过程分为数据采集阶段、数据处理及过滤阶段、入侵分析及检测阶段和报告及响应阶段共四个阶段。

数据采集阶段收集目标系统中的主机通信数据包和系统使用的数据信息。它是入侵检测的第一步。探测器通过监测接口捕获网络分组，采集的数据包括系统、网络、数据及用户获得的状态和行为。由放置在不同网段的传感器或不同主机的代理来收集包括系统和网络日志文件、网络流量、非正常的目录和文件改变、非正常的程序执行等信息。

数据处理及过滤阶段对采集到的数据进行分析和处理。如果有需要，对报文进行重组，并与标识典型入侵行为的规则进行比较。最常用的技术手段有三种，分别是模式匹配、统计分析和完整性分析。

入侵分析及检测阶段是整个入侵检测系统的核心阶段。根据数据采集阶段提供的数据，以及数据处理及过滤阶段产生的分析结果来判断是否发生入侵。如果通过数据分析，判断网络中可能发生了入侵行为，则通过命令和控制接口通知管理控制台。

在报告及响应阶段，如果检测到了入侵，管理控制台将发出警告，书写日志并采取某些行动，可能是重新配置路由器或防火墙、终止进程、切断连接、改变文件属性，也可能只是简单地警告。

15.2.3　入侵检测系统的分类

入侵检测被认为是防火墙之后的第二道安全闸门。入侵检测通过对入侵行为的过程和特征进行研究，使安全系统对入侵事件和入侵过程做出实时响应。根据输入数据的来源，把入侵检测系统分为三类。

1. 基于主机的入侵检测系统（HIDS）

基于主机的入侵检测系统输入数据来源于系统的审计日志，主要是针对该主机的网络实时连接，以及对系统审计日志进行智能分析和判断。基于主机的入侵检测系统通常安装在被重点检测的主机上，最适合检测内部人员的误用以及已经避开了传统的检测方法而渗透到网络中的活动。其优点是对分析“可能的攻击行为”非常有用，而且主机入侵检测系统通常比网络入侵检测系统误报率要低；缺点是主机入侵检测系统需要安装在需要保护的设备上，依赖于服务器固有的日志和监测能力。如果全面部署主机入侵检测系统，花费较大，只能选择部分主机进行保护，而那些未安装主机入侵检测系统的计算机将成为保护的盲点，入侵者可以把这些计算机作为攻击目标，并且主机入侵检测系统除了监测自身的主机外，根本不监测网络上的情况。

2. 基于网络的入侵检测系统（NIDS）

基于网络的入侵检测系统输入数据来源于网络信息流，通常部署在企业网络出口处或

内部关键子网边界等比较重要的网段内，检测流经整个网络的流量和网段中的各种数据包。它能够检测该网段上发生的网络入侵；也可以在检测到入侵后，通过向连接的交换机或防火墙发送指令，阻断后续攻击。网络入侵检测系统的优点是能够检测来自网络的攻击，能够检测到未授权的非法访问。它不需要改变服务器等主机配置，不需要安装额外软件，不会影响系统的性能。网络入侵检测系统安装方便，只要接通电源，做一些简单配置，再连接到网络上即可。部署网络入侵检测系统比主机入侵检测系统风险小很多，发生故障不会影响正常业务运行。其缺点是网络入侵检测系统只检查直连网段的通信，不能检测不同网段的网络包；并且网络入侵检测系统通常采用特征检测法，只能检测出普通攻击，很难实现复杂的、需要大量计算和分析时间的攻击检测。

3. 分布式入侵检测系统

分布式入侵检测系统是采用上述两种数据来源，能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统。一般为分布式结构，由多个部件组成。

15.2.4 入侵检测系统设备介绍

入侵检测系统 IDS 产品主要分为硬件和软件两种。这里讨论的主要是硬件产品。硬件产品和防火墙一起放置在机架上，而不是安装在操作系统中，可以很容易地把入侵检测系统 IDS 嵌入网络。一个硬件入侵检测系统 IDS 主要由传感器(Sensor)和控制台(Console)两部分组成。传感器的作用是采集数据，包括网络数据包、系统日志等，分析数据并生成安全事件。控制台的作用是中央管理，通常具有图形界面，便于控制和管理。IDS 设备的控制端称为 Console 口。IDS 的初始化配置是通过控制端口(Console)与计算机的串口(RS-232)相连，再通过 Windows 系统自带的超级终端程序进行配置。

入侵检测系统常用的检测方法有特征检测、统计检测和专家系统。据公安部计算机信息安全产品质量监督检验中心的报告，国内送检的入侵检测产品 95%是属于使用入侵模板进行模式匹配的特征检测产品，其他 5%是采用概率统计的统计检测产品与基于日志的专家知识库产品。市面上的入侵检测产品很多，如何判断一款入侵检测产品是否适合用户自己的需要，通常考虑的要点如表 15-1 所示。

表 15-1　入侵检测产品选购要点

最大可处理流量(包/秒，pps)	一般分为百兆位、千兆位
反躲避技术	能否有效检测分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等
产品的伸缩性	系统支持的传感器数目、最大数据库规模、传感器与控制台之间的通信带宽和对审计日志溢出的处理
产品支持的入侵特征数	不同厂商的计算方法不同，可参照国际标准
产品的响应方法	从本地、远程等多角度考察，是否支持防火墙联动
特征库升级及维护费用	特征库需要不断更新才能检测出新出现的攻击方法
是否通过了国家权威机构的评测	权威测评机构有国家信息安全测评认证中心、公安部计算机信息系统安全产品质量监督检验中心
是否有成功案例	了解产品的成功应用案例，必要时可进行实地考察和测试使用
产品的价格	性价比和保护系统的价值是更重要的因素

市面上的入侵检测产品很多，一些大型厂商如 IBM、思科、TippingPoint、Juniper 的产品，国内厂商如启明星辰、绿盟科技、天融信、H3C 的产品都是不错的选择，最终选择何种产品，需要用户视自己的实际情况而定。

15.3 方案设计

方案设计如表 15-2 所示。

表 15-2　方案设计

任务名称	入侵检测系统 IDS 的部署与配置
任务分解	1. IDS 的部署与配置 (1) 连接及登录 (2) IDS 系统设置 2. IDS 入侵检测规则配置 3. 基于自定义规则的 IDS 入侵检测 (1) 基础参数设置 (2) IP 参数设置 (3) ICMP 参数设置 (4) 阻断动作设置
能力目标	1. 能连接并登录入侵检测系统 IDS 2. 能查看系统信息 3. 能备份系统操作 4. 能诊断系统配置 5. 能设置入侵检测系统 IDS 自带的检测规则 6. 能使用入侵检测系统 IDS 根据规则检测入侵行为 7. 能自定义入侵检测系统 IDS 的检测规则 8. 能设置基础参数、关键字、IP 参数、TCP 参数、ICMP 参数和阻断动作 9. 能分析入侵检测日志 10. 能使用自定义规则检测入侵行为
知识目标	1. 掌握常见入侵检测系统的功能 2. 了解入侵检测的工作原理 3. 了解入侵检测系统的分类 4. 了解常见入侵检测设备 5. 了解 IDS 系统自带规则库中的各种攻击类型 6. 了解自定义规则内各参数含义 7. 熟悉入侵检测系统与防火墙的区别 8. 熟悉入侵检测系统与系统扫描器的区别 9. 掌握入侵检测系统 IDS 部署的位置
素质目标	1. 培养吃苦耐劳、实事求是、一丝不苟的工作态度 2. 树立较强的安全意识 3. 培养良好的职业道德 4. 培养分析能力和应变能力 5. 具有可持续发展能力

15.4 任务实施

为了完成本工作任务,又细分为以下 3 个子任务。

15.4.1 任务 1:IDS 的部署与配置

1. 任务目标

了解 IDS 设备的连接和简单设置;掌握 IDS 关于系统配置的常用功能模块,包括查看系统信息、备份系统操作和诊断系统配置等。

2. 工作任务

(1) 连接及登录;

(2) IDS 系统设置。

3. 工作环境

(1) 一台预装 Windows Server 2003/XP 的主机。

(2) 一台入侵检测系统 IDS。

4. 实施过程

(1) 连接及登录

① 单线接第 1 组蓝盾 IDS 设备的第一口,默认 IP 为 192.168.11.4,在 IE 输入 https://192.168.11.4;第 2 组蓝盾 IDS 第一口,默认 IP 为 192.168.12.4;在 IE 输入 https://192.168.12.4;第 3 组蓝盾 IDS 第一口,默认 IP 为 192.168.13.4;在 IE 输入 https://192.168.13.4;第 4 组蓝盾 IDS 第一口,默认 IP 为 192.168.14.4;在 IE 输入 https://192.168.14.4;第 5 组蓝盾 IDS 第一口,默认 IP 为 192.168.15.4;在 IE 输入 https://192.168.15.4;第 6 组蓝盾 IDS 第一口,默认 IP 为 192.168.16.4;在 IE 输入 https://192.168.16.4;第 7 组蓝盾 IDS 第一口,默认 IP 为 192.168.17.4;在 IE 输入 https://192.168.17.4;第 8 组蓝盾 IDS 第一口,默认 IP 为 192.168.18.4;在 IE 输入 https://192.168.18.4。统一用户密码为 admin/888888。

② 配置管理口 IP,单击“网络配置”→“网口设置”,配置 LAN2 口 IP,如图 15-1 所示。

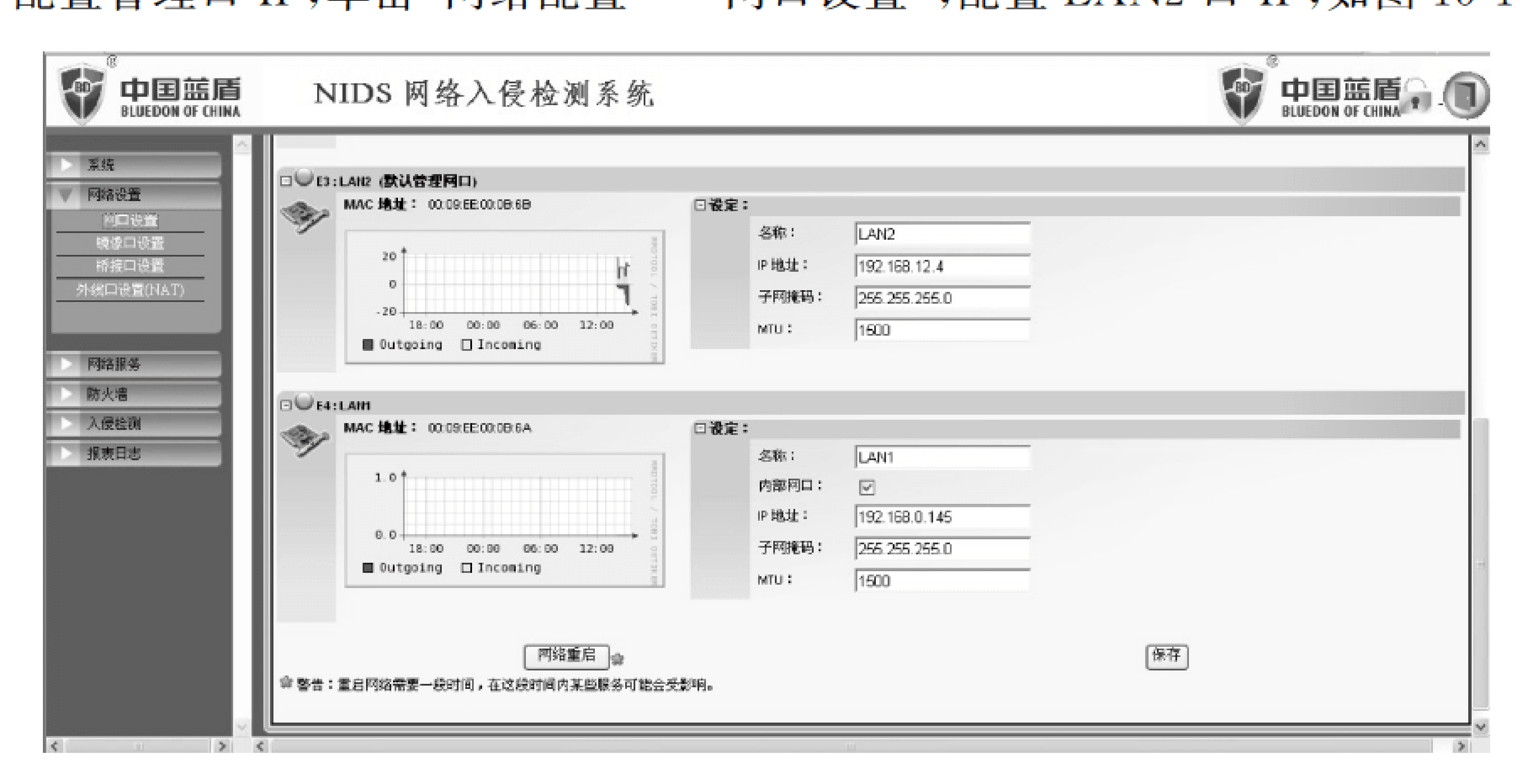


图 15-1 网口设置

③ 配置镜像口，单击“网络设置”→“镜像口设置”，为 LAN3 口选择镜像口，如图 15-2 所示。



图 15-2　镜像口设置

④ 配置 IDS 的管理设置，因为默认只有第一口能够访问，需做策略，让 LAN2 口能够访问管理。单击“系统”→“管理设置”，如图 15-3 所示。



图 15-3　管理设置

（2）IDS 系统设置

① 单击“系统”→“系统信息”→“设备状态”进入设备状态页面。该页面显示系统信息、网络接口信息、系统服务等，如图 15-4 所示。



图 15-4　设备状态

参数定义：

- 系统信息：系统 CPU、内存及硬盘的实时使用情况。
- 网络接口信息：与设备相连各网口的 IP 地址，以及数据包收发比特数。
- 系统服务：各项服务是否打开。表示此服务已经打开，表示服务未打开。

② 单击“系统”→“系统维护”→“配置备份”进入备份恢复页面，如图 15-5 所示。

备份恢复 | 系统更新 | 系统时间 | 关闭系统

⊟备份文件列表

选择分页大小 20　　1 /1　　2条记录　　刷新

序号	备份文件	大小	日期	描述	
1	bluedon	5 KB	20100408 181125		
2	Bluedon-Default	7 KB	20000101 000000		

制作　上传　下载　恢复　删除

图 15-5　备份恢复

参数定义：

- 制作：将系统已做好的策略保存下来，备份成配置文件。
- 上传：将下载到本地的配置文件上传到设备，才能选择进行故障恢复。
- 下载：将配置文件下载到本地机器上，防止系统意外出现事故，是一种防范机制。
- 恢复：可以将下载到本地的配置文件在设备出现故障时上传到设备，进行恢复。
- 设置：该项是设置设备的启动服务选项，一般配置为默认。

③ 单击“系统”→“系统维护”→“关闭系统”关闭设备页面，如图 15-6 所示。



图 15-6　关闭系统

- 立即：立即执行“重启”和“关闭”设备。
- 之后：在之后的 5 分钟至 1 小时之内的某个特定时间“重启”和“关闭”设备。
- 定时：通过设置定时时间，能在当天的特定时间“重启”和“关闭”设备。

④ 单击“系统”→“系统工具”→“配置测试”进入测试结果页面，如图 15-7 所示。该页面显示对系统配置的诊断，以便检查配置情况。

⑤ 单击“系统”→“系统工具”→“IP 工具”，该页面用于测试一个 IP 或者主机能否正常通信，如图 15-8 所示。

⑥ 输入 IP 地址，然后单击“执行”按钮，结果如图 15-9 所示。

⑦ 在“工具”下拉列表中选择 whois，然后单击“执行”按钮，结果如图 15-10 所示。

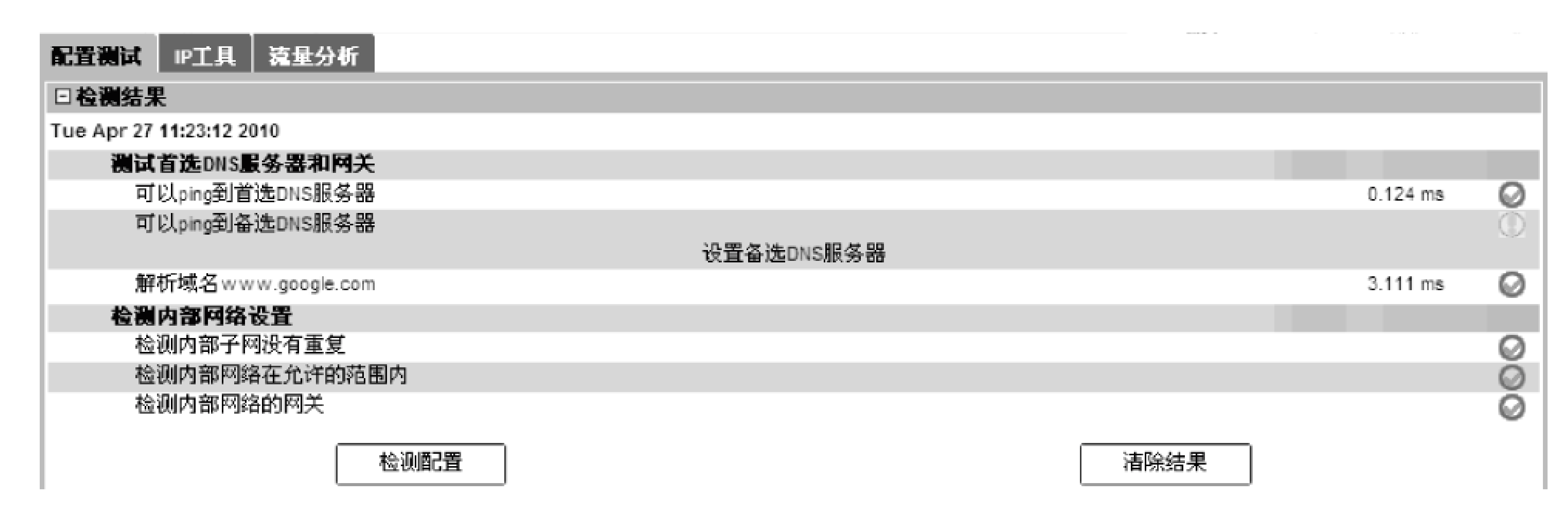


图 15-7　配置测试结果

配置测试　IP工具　流量分析

工具	Ping
出口IP或网口	
IP地址或主机名	

执行

图 15-8　IP 工具

配置测试　IP工具　流量分析

工具	Ping
出口IP或网口	
IP地址或主机名	192.168.228.254

执行

192.168.228.254 (反向查找失败)

```
PING 192.168.228.254 (192.168.228.254) 56(84) bytes of data.
64 bytes from 192.168.228.254: icmp_seq=1 ttl=255 time=4.84 ms
64 bytes from 192.168.228.254: icmp_seq=2 ttl=255 time=4.11 ms
64 bytes from 192.168.228.254: icmp_seq=3 ttl=255 time=3.14 ms
64 bytes from 192.168.228.254: icmp_seq=4 ttl=255 time=3.14 ms
64 bytes from 192.168.228.254: icmp_seq=5 ttl=255 time=7.71 ms

--- 192.168.228.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4041ms
rtt min/avg/max/mdev = 3.143/4.593/7.715/1.687 ms
```

图 15-9　IP 工具运行

配置测试　IP工具　流量分析

工具	whois
出口IP或网口	
IP地址或主机名	www.google.com

执行

66.249.89.104 (nrt04s01-in-f104.1e100.net)

```
BW whois 3.4 by Bill Weinman (http://whois.bw.org/)
Copyright 1999-2003 William E. Weinman
Request: 66.249.89.104
unable to connect to whois.arin.net (111: Connection refused)
```

图 15-10　IP 工具运行结果

15.4.2 任务 2：IDS 入侵检测规则配置

1. 任务目标

了解 IDS 系统自带检测规则库中的各种攻击类型，初步掌握对用户自定义规则的配置。本实验主要介绍 IDS 自带的检测规则库及用户自定义规则的配置。IDS 的检测规则、关联规则都需要根据网络的实际情况来配置。当出现入侵时，所有的入侵行为数据都会在 IDS 服务器内根据规则进行检测(捕获、拆分、分析、匹配)。

2. 工作任务

系统自带检测规则设置。

3. 工作环境

(1) 一台预装 Windows Server 2003/XP 的主机。

(2) 一台入侵检测系统 IDS。

4. 实施过程

(1) 单击“入侵检测”→“检测规则”，该页面显示所有 IDS 系统自带检测规则，用户可以查看已经勾选的规则库，或选择规则库。系统会定时自动下载、更新规则库，使用户得到及时的保护。用户也可上传自定义补丁更新规则库，如图 15-11 所示。



图 15-11 “检测规则”窗口

建议只勾选必要的选择，以提高检测的速率和性能。例如，如果内部网络中没有数据库服务器，则不必勾选数据库选项下的规则库。一般情况下，勾选的规则越多，对进、出数据包的检测匹配耗时越长，降低了 IDS 设备处理性能。

(2) 单击“入侵检测”→“检测规则”→“规则设置”，将分类罗列已有规则及其危害等级，并可对各规则进行编辑，选择对违反该规则的行为警报(Alert)、通过(Pass)，或者拒绝(Reject)，如图 15-12 所示。



图 15-12　“规则设置”窗口

(3) 单击“入侵检测”→“检测规则”→“自定义规则”，让用户自行定义入侵检测规则，如图 15-13～图 15-19 所示。

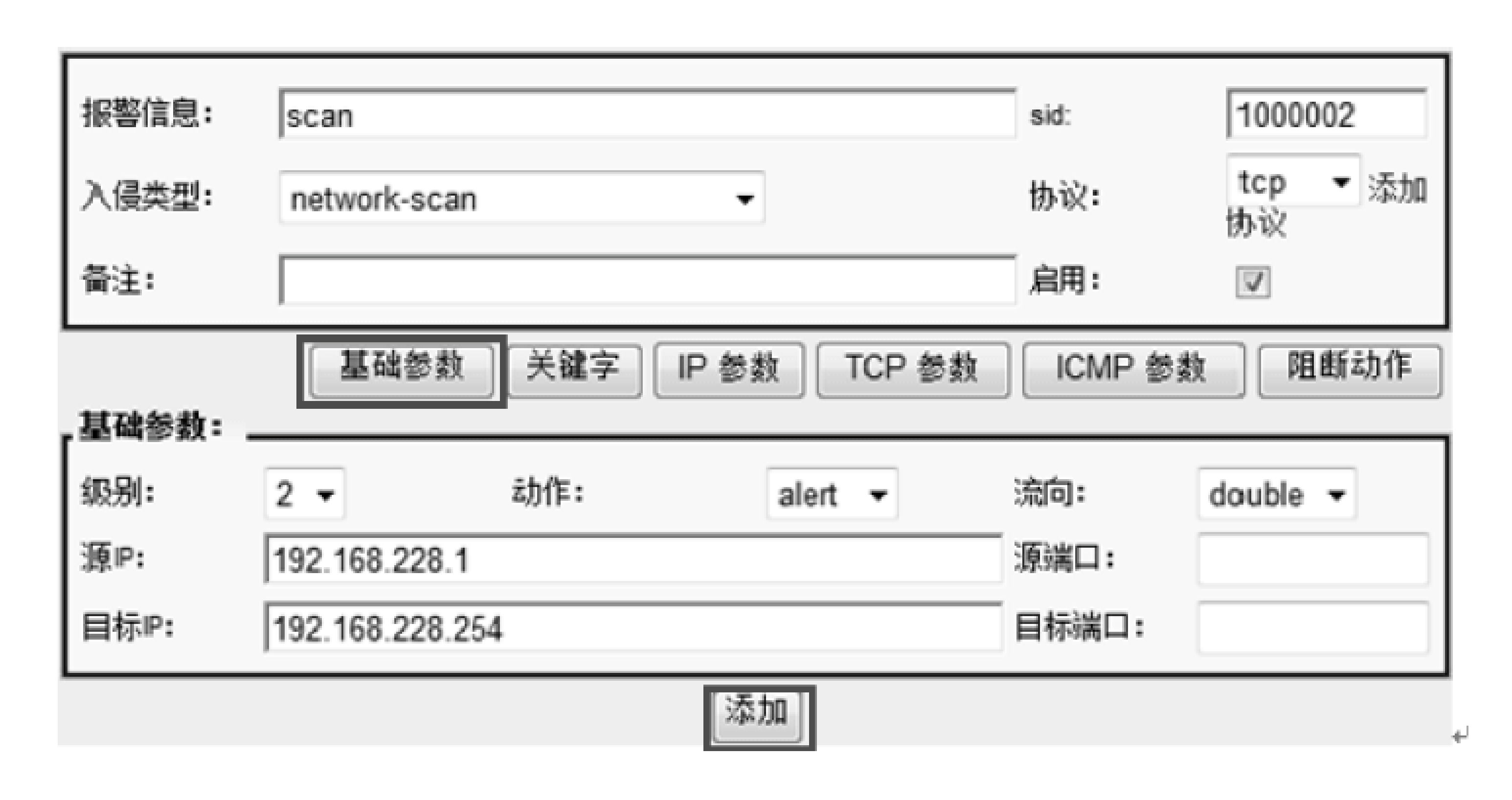


图 15-13　“基础参数”配置

参数定义：

- 报警信息：指触发该检测事件时，报警的内容。
- sid：指事件的编号。为避免与系统自带规则库的事件编号有冲突，请使用 1000001 开始的编号。
- 入侵类型：对入侵事件的归类，请选择最接近的归类。
- 协议：对入侵数据流的协议定义。
- 基础参数：对该事件的基础数据描述，如报警级别、采取动作、流向(单向(single)、双向(double))、源地址、源端口、目标地址、目标端口等与协议无关的基础参数。



图 15-14 “内容关键字”配置

参数定义：

- 内容关键字：定义入侵数据流中的特征码，以更准确地判断出入侵行为。
- offset：content 选项的修饰符，设定开始搜索的位置。
- depth：content 选项的修饰符，设定搜索的最大深度。
- distance：使用 content 时，模式匹配间至少有 N 个字节存在。
- within：使用 content 时，模式匹配间最多有 N 个字节存在。
- rawbytes：允许规则查看 Telnet 解码数据来处理不常见的数据。

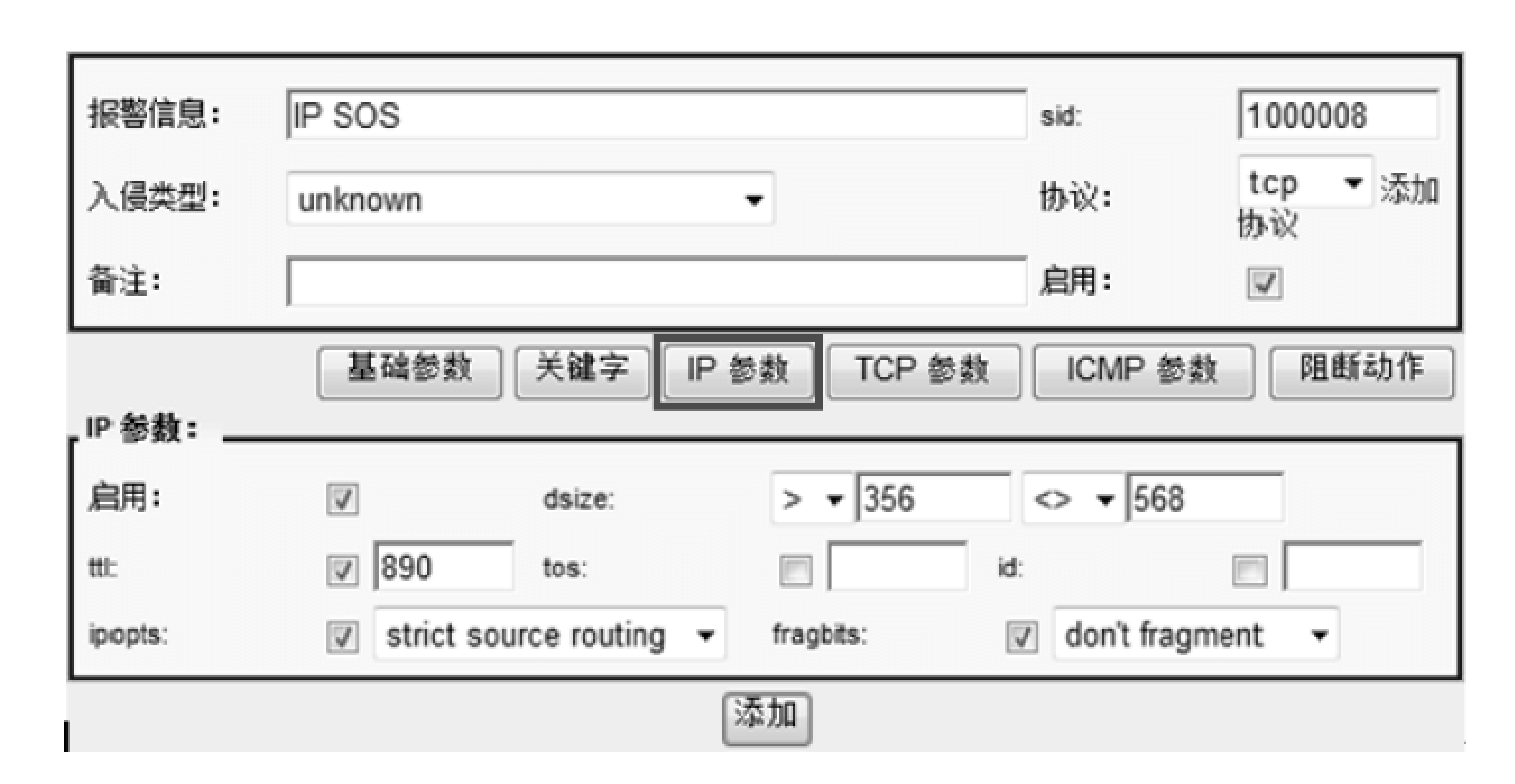


图 15-15 “IP 参数”配置(1)

参数定义：

- IP 参数：如果在“协议”项目选择了 IP 协议，可以在这里设定关于该事件更具体的 IP 参数。
- dsize：检查包的数据部分大小。
- ttl：检查 IP 头的 TTL 的值。
- tos：检查 IP 头的 TOS 域的值。
- id：检查 IP 头的分片 ID 值。
- ipopts：检查 IP 头的 Option 域。
- fragbits：检查 IP 头的分片标志位。



图 15-16　“TCP 参数”配置

参数定义：

- TCP 参数：如果在“协议”项目选择了 TCP 协议，可以在这里设定关于该事件更具体的 TCP 参数。
- seq：检查 TCP 顺序号的值。
- ack：检查 TCP 应答(Acknowledgement)的值。
- window：检查 Window 的值。
- flags：检查 TCP Flags 的值。
- fin：检查 FIN 的值。
- syn 检查 SYN 的值。
- rst：检查 RST 的值。



图 15-17　“ICMP 参数”配置(1)

参数定义：

- ICMP 参数：如果在“协议”项目选择了 ICMP 协议，可以在这里设定关于该事件的更具体的 ICMP 参数。
- id：检查 ICMP Echo ID 的值。
- seq：检查 ICMP Echo 顺序号的值。
- itype：检查 ICMP Type 的值。
- icode：检查 ICMP Code 的值。



图 15-18 “阻断动作”配置(1)

参数定义：

- 阻断动作：对此入侵事件采取阻断动作。
- 断开 TCP：rest dest 是向发送方发送 TCP-RST 数据包，reset source 是向接收方发送 TCP-RST 数据包，reset both 是向收发双方发送 TCP_RST 数据包。
- 断开 HTTP：block 是关闭连接并且发送一个通知，warm 是发送明显的警告信息，msg 是把 MSG 选项的内容包含进阻塞通知信息中。
- 断开 ICMP：icmp net 是向发送方发送 ICMP_NET_UNREACH，icmp host 是向发送方发送 ICMP_HOST_UNREACH，icmp port 是向发送方发送 ICMP_PORT_UNREACH，icmp all 是向发送方发送上述所有的 ICMP 数据包。



现有规则：

ID	名称	SID	级别	动作	类型	协议	流向	内容关键字	启动	选择
					备注					
1	icmp cut	1000015	3	alert	icmp-event	tcp	single		☑	☐

图 15-19 启动规则

(4) 单击“入侵检测”→“检测规则”→“统计规则”。统计规则指的是对一段时间内重复出现的低级别事件进行统计综合报警，这样可以减少不必要的报警次数。比如，对于“ICMP Windows PING”事件，如果需要在 60s 内重复出现 10 次才报警，配置如图 15-20 所示。



图 15-20 “统计规则”配置

其中，GID和SID可以通过查询得到。

15.4.3　任务3：基于自定义规则的IDS入侵检测

1. 任务目标

了解自定义规则内各参数的含义；掌握分析入侵检测日志的方法；根据实际需要，允许有经验的高级用户自定义入侵规则。

本实验主要介绍IDS系统的自定义检测规则的配置方式，包括对基础参数、关键字、IP参数、TCP参数、ICMP参数和阻断动作的介绍及设置。通过实验，能更清楚地了解规则制定、入侵检测过程、事件记录、处理入侵的一系列过程。自定义规则使得规则的制定有更大的扩展性和自由性，但对用户的操作水平有更高的要求。

2. 工作任务

(1) 基础参数设置；

(2) IP参数设置；

(3) ICMP参数设置；

(4) 阻断动作设置。

3. 工作环境

(1) 一台预装Windows Server 2003/XP的主机。

(2) 一台入侵检测系统IDS。

4. 实施过程

单击"入侵规则"→"检测规则"，启动入侵检测规则，然后勾选自定义规则，再单击"保存"按钮，如图15-21所示。



图15-21　"自定义规则"配置

(1) 基础参数设置

① 单击"入侵规则"→"检测规则"→"自定义规则"→"基础参数"，配置如图15-22所示。

② 从下拉列表中选择TCP协议后，单击"启用"。然后单击"添加"按钮，得到一条针对所有未知入侵的检测规则Intrusion_Info，如图15-23所示。

③ 单击"报表日志"→"系统日志"→"入侵检测日志"。扫描是最常见的入侵行为之一。当扫描操作发生时，Intrusion_Info日志会实时记录下这一入侵行为，以供用户做出相应的防范。

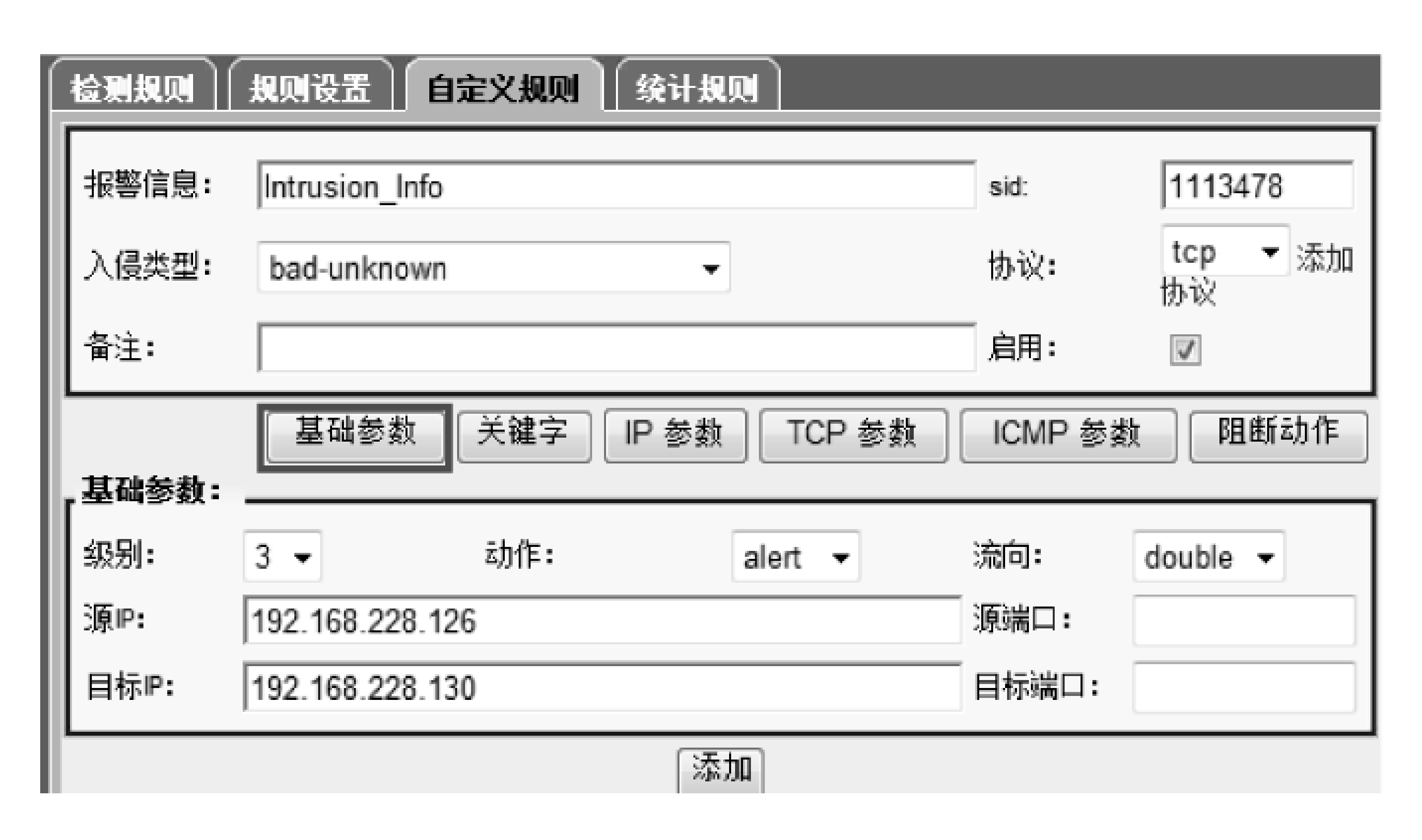


图 15-22 “基础参数”配置



图 15-23 添加规则

(2) IP 参数设置

① 单击“入侵规则”→“检测规则”→“自定义规则”→“IP 参数”，参照图 15-24 填入要检测的项。在 ttl 项填入“64”作为参考值，选择“启用”，然后单击“添加”按钮，如图 15-24 所示，得到一条名称为 IP_info 的检测规则，如图 15-25 所示。

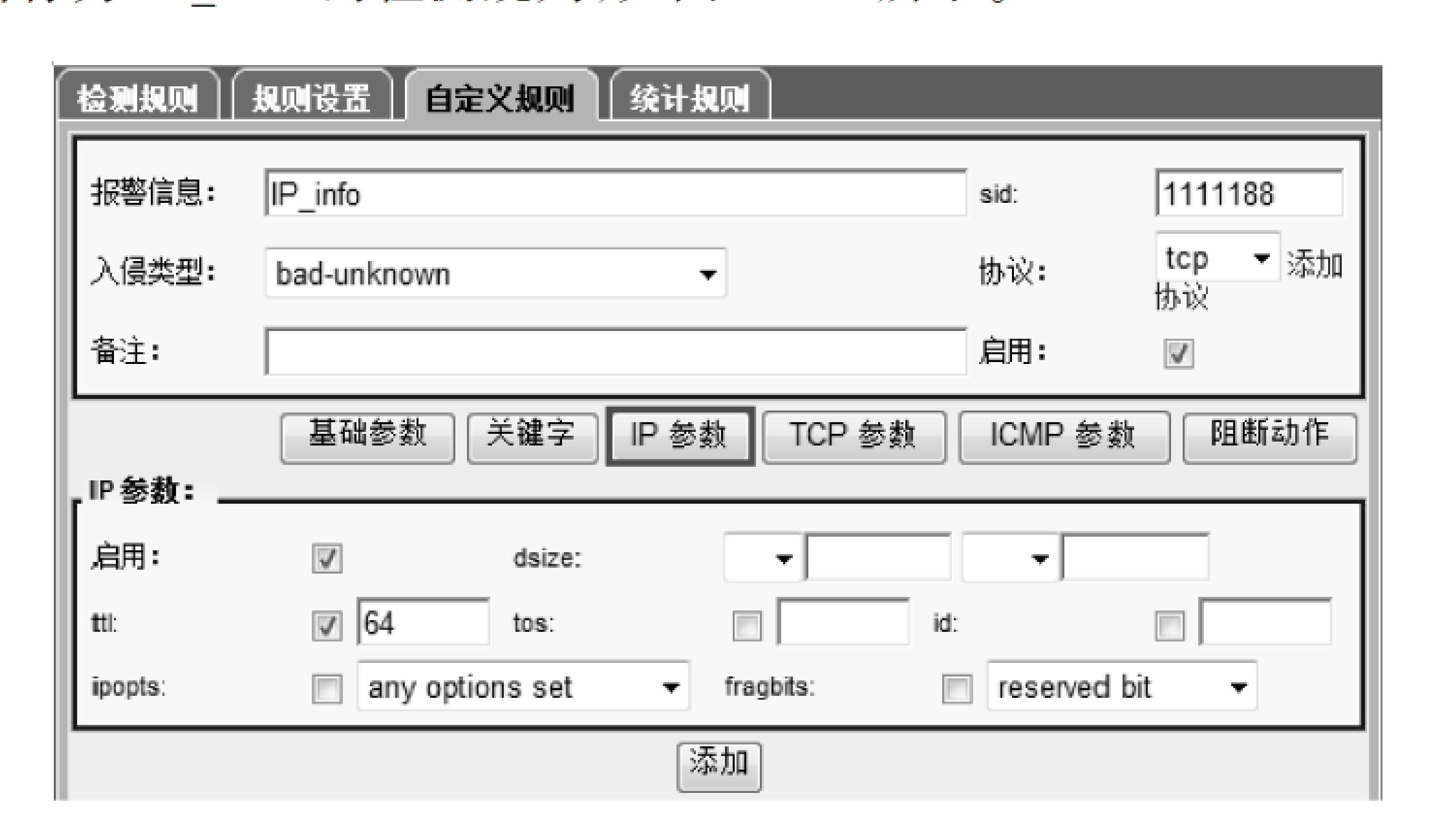


图 15-24 “IP 参数”配置(2)



图 15-25 IP_Info 检测规则

② 单击“报表日志”→“系统日志”→“入侵检测日志”，当满足检测规则的操作发生时，IP_info 日志就记录下该行为。

（3）ICMP 参数设置

① 单击“入侵规则”→“检测规则”→“自定义规则”→“ICMP 参数”，参照图 15-26 填入要检测的项。这里直接启用检测 ICMP 项来检测 ping 工具，选择“启用”，再单击“添加”按钮，如图 15-26 所示，得到一条名称为 ICMP_info 的检测规则，如图 15-27 所示。

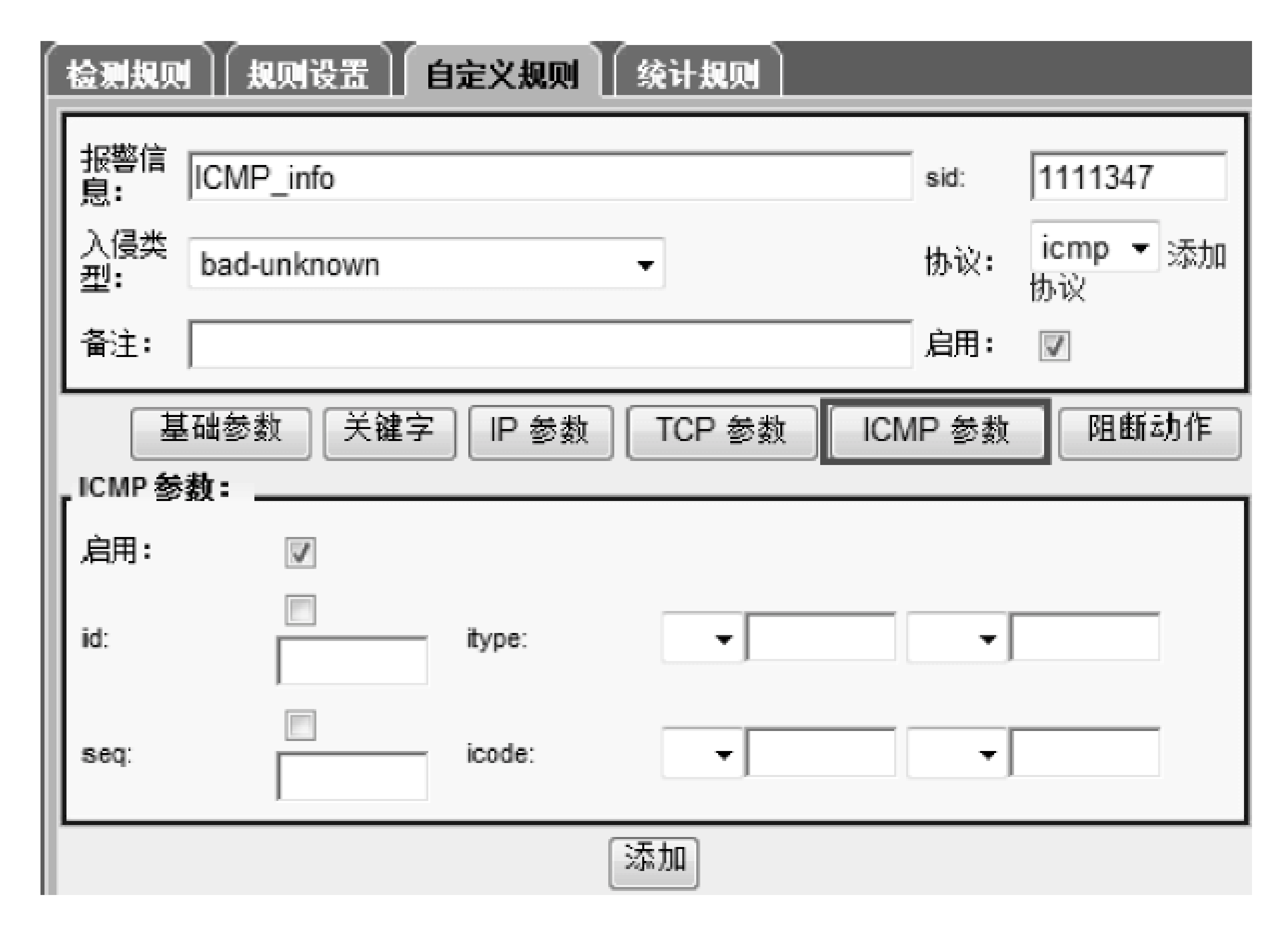


图 15-26　“ICMP 参数”配置(2)



图 15-27　ICMP_Info 检测规则

② 单击“报表日志”→“系统日志”→“入侵检测日志”。ping 操作时，记录下来名称为 ICMP_info 的日志，如图 15-28 所示。

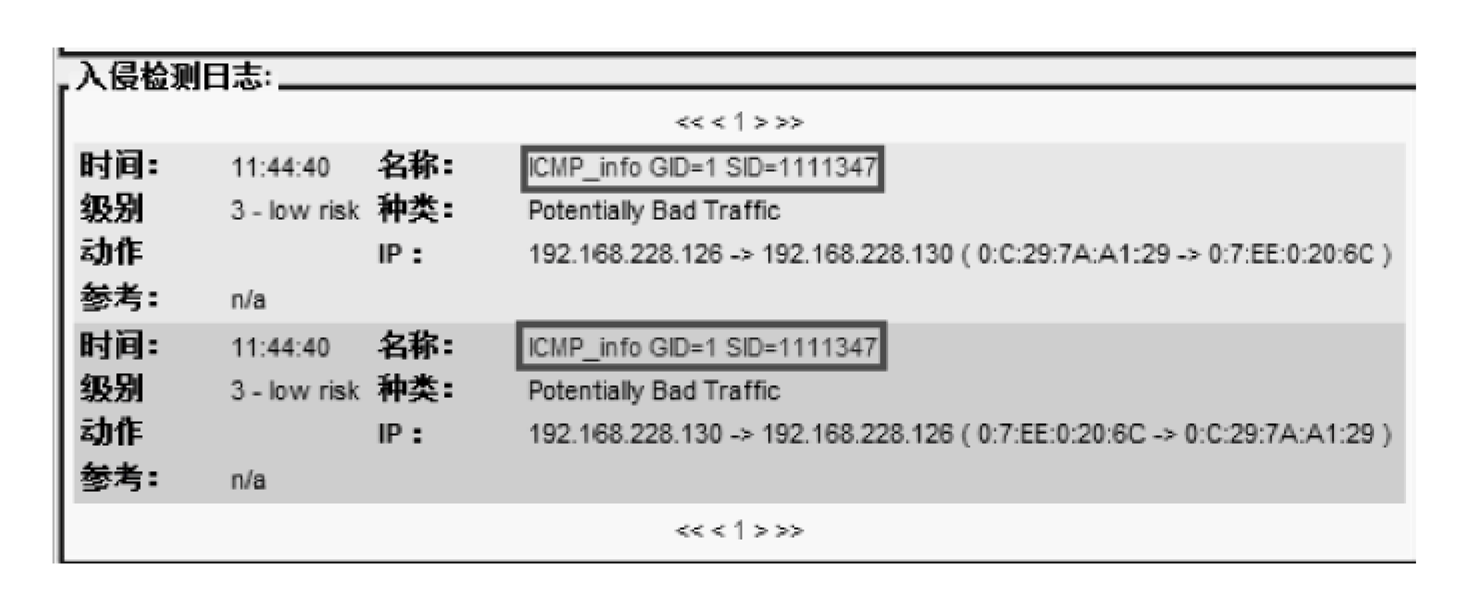


图 15-28　入侵检测日志(1)

（4）阻断动作设置

① 单击“入侵规则”→“检测规则”→“自定义规则”→“阻断动作”，参照图 15-29 所示填入所要检测的项。这里选择“断开 ICMP”，得到一条名称为 Cutoff_Info 的检测规则，如图 15-30 所示。

检测规则 规则设置 自定义规则 统计规则

报警信息：Cutoff_Info sid：1111490

入侵类型：bad-unknown 协议：icmp 添加协议

备注： 启用：

基础参数 关键字 IP 参数 TCP 参数 ICMP 参数 阻断动作

阻断动作：

断开TCP： reset dest reset source reset both

断开HTTP： block warm msg

断开ICMP： icmp net icmp host icmp port icmp all

添加

图 15-29 “阻断动作”配置(2)



图 15-30 Cutoff_Info 检测规则

② 单击“报表日志”→“系统日志”→“入侵检测日志”。当在系统中执行阻断操作时，会记录下名称为 Cutoff_Info 的日志，如图 15-31 所示。

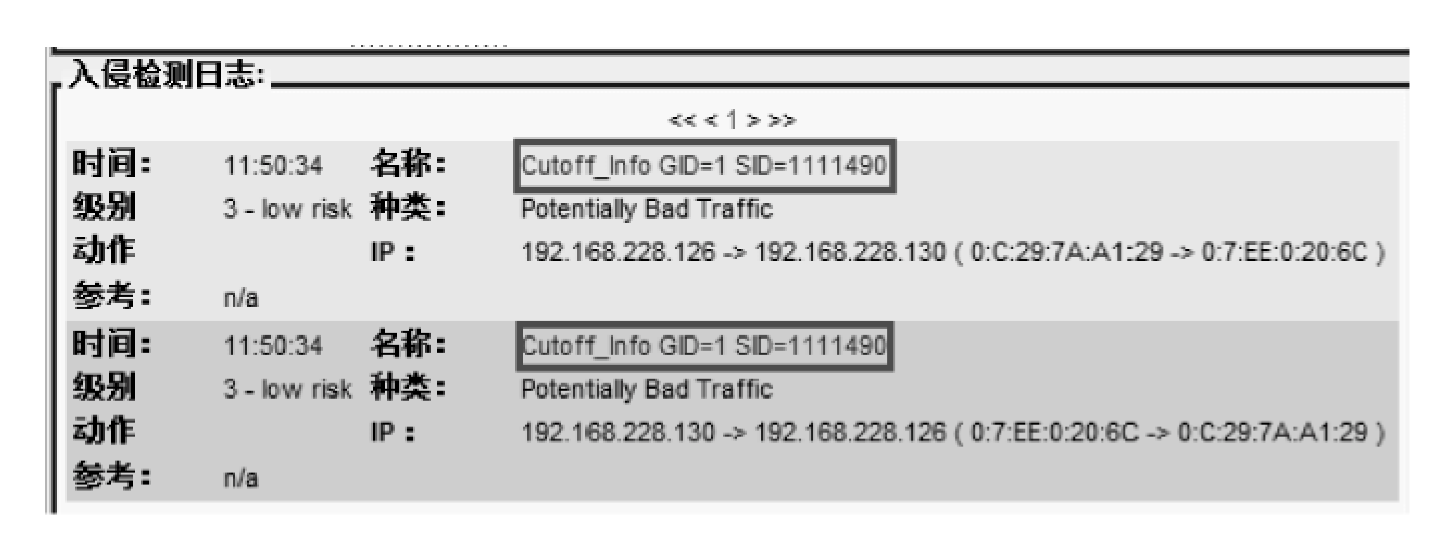


图 15-31 入侵检测日志(2)

15.5 常见问题解答

1. 入侵检测系统 IDS 与防火墙有什么不同?

答：如果把防火墙比作一栋大楼的门锁，那么入侵检测系统 IDS 就是这栋大楼里的监视系统。一旦有小偷爬窗进入大楼或者内部人员有越界行为，只有实时监控系统才能发现情况并发出警告。通过在网络中安装防火墙，可以阻挡一般性的网络攻击行为；采用入侵检测系统 IDS，可以对越过防火墙的攻击行为，以及来自网络内部的违规操作进行检测和响应，相当于为网络提供第二道保护机制。入侵检测系统多安装在防火墙之后，对网络活动进行实时检测。在多数情况下，由于可以记录和禁止网络活动，所以入侵检测系统是防火墙的延续，可以和防火墙以及路由器配合工作。

2. 入侵检测系统 IDS 与系统扫描器有何不同?

答:系统扫描器是根据攻击特征数据库来扫描系统漏洞,它更关注配置上的漏洞,而不是实时进出主机的流量。在遭受攻击的主机上,即使正在运行扫描程序,也无法识别这种攻击。IDS 扫描当前网络的活动,监视和记录网络流量,根据定义好的规则过滤从主机网卡到网线上的流量,提供实时报警。系统扫描器只检测主机上先前设置的漏洞,而 IDS 监视和记录网络流量。如果在一台主机上运行 IDS 和扫描器,配置合理的 IDS,会发出很多警报。

3. 入侵检测系统 IDS 与入侵防御系统 IPS 有何不同?

答:入侵防御系统与入侵检测系统有些类似,但是 IPS 一般是立刻采取行动阻止威胁,例如及时阻止某个 IP 地址或用户的访问,而不仅仅是简单地发出警报。IDS 是被动采取行动,IPS 是主动响应系统。

4. 入侵检测系统 IDS 部署的位置在哪里?

答:入侵检测系统 IDS 应当挂接在所有关注流量都必须流经的链路上。关注的流量包括来自高危网络区域的访问流量和需要进行统计、监视的网络报文。因此,IDS 在交换式网络中的位置一般选择为尽可能靠近攻击源,尽可能靠近受保护资源,通常连接在服务器区域交换机上,或者在重点保护网段的局域网交换机上。

15.6 过关练习

选择题

1. 以下关于入侵检测系统的描述中,错误的是(　　)。
   A. 入侵检测是一种主动保护网络免受攻击的安全技术
   B. 入侵检测是一种被动保护网络免受攻击的安全技术
   C. 入侵检测系统能够对网络活动进行监视
   D. 入侵检测能简化管理员的工作,保证网络安全运行
2. 按照检测数据的来源,可将入侵检测系统(IDS)分为(　　)。
   A. 基于主机的 IDS 和基于网络的 IDS
   B. 基于主机的 IDS 和基于域控制器的 IDS
   C. 基于服务器的 IDS 和基于域控制器的 IDS
   D. 基于浏览器的 IDS 和基于网络的 IDS
3. (　　)不属于将入侵检测系统部署在 DMZ 中的优点。
   A. 可以查到受保护区域主机被攻击的状态
   B. 可以检测防火墙系统的策略配置是否合理
   C. 可以检测 DMZ 被黑客攻击的重点
   D. 可以审计来自 Internet 上对受到保护网络的攻击类型

工作任务十六

VPN服务器的配置与管理

16.1 用户需求与分析

很多企业采用了网络防火墙来加强安全措施，但是防火墙不容易做到数据加密、用户认证等。有些系统采用软件加密，但软件加密会消耗大量用户服务器的资源，影响系统的响应速度。由于 VPN 比租用专线更加便宜、灵活，所以有越来越多的公司采用 VPN，连接在家工作和出差在外的员工，以及替代连接分公司和合作伙伴的标准广域网。VPN 建在互联网的公共网络架构上，通过“隧道”协议，在发送端加密数据，在接收端解密数据，以保证数据的私密性。

16.2 预 备 知 识

16.2.1 VPN 的功能

VPN(Virtual Private Network，虚拟专用网)可以实现不同网络的组件与资源之间的相互连接。虚拟专用网能够利用 Internet 或其他公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。虚拟专用网允许远程通信，出差人员或企业分支机构可以使用 Internet 等公共互联网络的路由基础设施以安全的方式与位于企业局域网内的企业服务器建立连接。虚拟专用网络对用户端透明，用户就像使用一条专用线路在客户计算机和企业服务器之间建立点对点连接，进行数据的传输，并且数据进行了加密处理，保护了数据的机密性及完整性。目前，VPN 主要采用隧道技术(Tunneling)、加/解密技术(Encryption/Decryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication)来保证内部数据通过 Internet 安全传输。

VPN 的技术优势如下：

(1) 安全性。VPN 利用隧道技术对原有协议重新封装，并提供加密、数据验证、用户验证等一系列安全防护措施，保证了数据通过不安全的公共网络得到安全的传输。

(2) 经济性。与专线技术相比，VPN 技术降低了费用，在原有网络连接的条件下提供了比专线技术更安全的数据保护机制。

(3) 扩展性。与专线技术相比，VPN 技术通过在用户端的配置就可以灵活地扩展，不需要新的申请或投入。

16.2.2 VPN 的分类

1. VPN 的应用分类

(1) 远程接入 VPN 应用模式：远程接入 VPN，实现出差员工或家庭办公应用等移动用

户安全访问企业网络的应用。

(2) Intranet VPN 应用模式：Intranet VPN 用于跨地区的企业总部与分支机构内部网络的安全互联。

(3) Extranet VPN 应用模式：Extranet VPN 用于企业与客户、合作伙伴之间建立安全的网络互联。

2. VPN 网络结构的分类

(1) VPN 的远程访问结构：用于提供远程移动用户对企业内部网络资源的安全访问，即 Access VPN。单机通过公共网络利用隧道技术连接到企业网络，成为网络中的一个连接点，这种结构又称为点到站点、桌面到网络结构。

(2) VPN 的网络互联结构：用于企业总部网络和分支机构网络的内部网络之间的安全互联，即 Intranet VPN 或 Extranet VPN。保护网络互联时在公共网络传输过程中的数据安全，同时防止非法访问内部网络资源。这是一种网络到网络，也称为站点到站点的结构。

(3) VPN 的点对点通信结构：用于企业内部网的两台主机之间的安全通信，即单机到单机结构。

3. VPN 所采用的隧道协议

从 VPN 采用的隧道协议所处的网络层次来看，PPTP、L2P 和 L2TP 等 VPN 协议工作在 TCP/IP 协议簇的第二层(数据链路层)，IPSec、GRE 等协议工作在 TCP/IP 协议簇的第三层(网络层)，SSL/TLS VPN 协议工作在 TCP/IP 协议簇的第四层(传输层)，MPLS 协议跨越第二层和第三层。L2TP、IPSec 是第二层和第三层配合的隧道协议。

4. VPN 接入方式分类

一般的企业都有自己的局域网络，多是通过光纤连接到互联网。对于单个出差用户或家庭用户，是通过拨号(如 ADSL)连接到 ISP，这种方式建立的 VPN 称为拨号接入 VPN，也称为 VPDN。在路由器上，用 vpdn enable 命令启用 VPDN 功能。

16.2.3　VPN 典型协议

1. SSL VPN

SSL VPN 是一种新兴的应用层 VPN 技术。SSL 协议定义了完整的安全机制，对用户数据的完整性和私密性都有完善的保护。常见 SSL VPN 网关提供了四种 SSL VPN 接入方式以适应不同用户需求，包括 Web 转发方式、端口转发方式、文件共享方式和全网接入方式，其接入功能分别由不同的功能模块完成，同时具备强大的访问控制、权限管理、细粒度审计和日志记录等功能。

2. IPSec VPN

IPSec(IP 安全协议)是由 IETF 制定的，在网络层提供安全的一组协议，用于保证数据报在网络上传输时的私有性、完整性、真实性和防重放。

(1) 私有性(Confidentiality)：在传输数据包之前将其加密，以保证数据的私有性。

(2) 完整性(Integrity)：在目的地验证数据包，以保证数据包在传输过程中没有被修改。

(3) 真实性(Authentication)：验证数据源，以保证数据来自真实的发送者。

(4) 防重放(Anti-replay):防止恶意用户通过重复发送捕获到的数据包所进行的攻击,即接收方会拒绝旧的或重复的数据包。

IPSec 安全体系结构包括 AH(身份认证头)协议、ESP(封装安全负载)协议和 ISAKMP(密钥管理)协议。其中,AH 协议提供了源身份认证和数据完整性,但是没有提供保密性;ESP 协议提供了数据完整性、身份认证和保密性;ISAKMP 协议提供双方交流时的共享安全信息。

IPSec 主要有传输模式和隧道模式两种工作模式。其中,传输模式是系统默认的 IPSec 工作模式,主要应用于两台主机之间(即端对端之间)数据安全通信的场合,此时 AH 头或 ESP 头被插入在原始 IP 头和传输层报头(TCP 头或 UDP 头)之间。隧道模式主要应用于两个网络之间进行数据安全通信的场合。例如,将两台路由器(或网关、防火墙等)分别指派为隧道终结点,此时整个原始 IP 包被封装在一个新的 IP 包中,并在新 IP 头和原始 IP 头之间插入 AH 头或 ESP 头。

IPSec 的密钥管理包括密钥的确定和分发。IPSec 支持手动密钥分配和自动密钥分配两种管理方式。手动密码分配方式的优点是简单,缺点是安全性较低;自动密钥分配的优点是安全性较高,缺点是算法实现、密钥管理等较复杂。Windows Server 2003 系统默认 IPSec 安全策略包含客户端(仅响应)、服务器(请求安全)和安全服务器三种。但在某台计算机上,最多只能指派一条 IPSec 策略。在 CMD 窗口中,启动 IPSec 服务的命令是 net start policyagent。若要使用"IP 安全监视器"控制台查看 IPSec 策略指派情况,必须在 MMC 管理单元中进行相关操作。一条 IPSec 安全策略的基本组件包括:要匹配的通信类型,当通信匹配时做些什么,隧道或传输模式的选择,身份验证方法和规则应用于哪种连接类型。

源主机在向目标主机发送安全数据报之前,需要先握手并建立网络层逻辑连接。该逻辑通道称为安全协议(SA)。SA 是 IPSec 的基础,也是 IPSec 的本质。SA 是通信对等体间的约定,例如使用哪种协议(AH、ESP,还是两者结合)、协议的操作模式(传输模式还是隧道模式)、加密算法(DES 等)、特定流中保护数据的共享密钥及密钥的生存周期。SA 定义的逻辑连接是一个单工连接,即连接是单向的。SA 唯一定义为一个三元组,包括安全协议(AH 或 ESP)标识符、单工连接的源 IP 地址和称为安全参数索引(SPI)的 32 位连接标识符。AH 头在原有 IP 数据包数据(TCP 或 UDP 段)和原 IP 头之间。对于 IP 数据报头的协议字段,值 50 表明数据报包含 ESP 头和 ESP 尾,值 51 表明数据报包含 AH 头。

3. PPTP 和 L2TP

点对点隧道协议(PPTP)是一种网络协议,它通过跨越基于 TCP/IP 的数据网络创建 VPN,实现了从远程客户端到专用企业服务器之间数据的安全传输。PPTP 支持通过公共网络(如 Internet)建立按需的、多协议的虚拟专用网络。PPTP 允许加密 IP 通信,然后在要跨越公司 IP 网络或公众 IP 网络(如 Internet)发送的 IP 头中对其进行封装。

第二层隧道协议(L2TP 协议)是一种基于 PPP 协议的二层隧道协议,其报文封装在 UDP 之上,使用 UDP 1701 端口。L2TP 没有任何加密措施,通常和 IPSec 协议结合使用,提供隧道验证。它是典型的被动式隧道协议,可从客户端或访问服务器端发起 VPN 连接。在 L2TP 构建的 VPN 网络中,主要有 L2TP 访问集中器(LAC)和 L2TP 网络服务器(LNS)两种关键的网络设备。其中,LAC 支持客户端的 L2TP,用于发起呼叫、接收呼叫和建立隧道,是一种附属在网络上的具有 PPP 端系统和 L2TPv2 协议处理能力的设备。LNS 是 PPP

端系统上用于处理 L2TP 服务器端部分的软件,是所有隧道的终点。LNS 终止所有的 PPP 流。在传统的 PPP 连接中,用户拨号连接的终点是 LAC;L2TP 使得 PPP 的终点延伸到 LNS。

16.3　方案设计

方案设计如表 16-1 所示。

表 16-1　方案设计

任务名称	VPN 服务器的配置与管理
任务分解	1. 远程访问 VPN 的配置 (1) 配置 VPN 服务器 (2) VPN 网络客户端的设置 (3) VPN 连接检测 2. 点对点通信 VPN 连接的配置 (1) 创建 IPSec 策略 (2) 建立从 A 到 B 的筛选器列表 (3) 建立从 B 到 A 的筛选器列表 (4) 为 A 到 B 隧道配置规则 (5) 为 B 到 A 隧道配置规则 (6) 将新的 IPSec 策略指派 3. VPN 服务器的系统管理 (1) 连接及登录 (2) VPN 服务器的系统管理
能力目标	1. 能配置 VPN 服务器 2. 能对 VPN 网络的客户端进行设置 3. 能测试 VPN 连接 4. 能创建 IPSec 策略 5. 能创建筛选器列表和隧道配置规则 6. 能将新的 IPSec 策略指派 7. 能连接并登录 VPN 服务器 8. 能对 VPN 服务器进行系统管理
知识目标	1. 熟悉 VPN 的功能 2. 了解 VPN 的技术优势 3. 了解 VPN 的应用分类、网络结构分类和接入方式分类 4. 了解 VPN 的典型协议 SSL VPN、IPSec VPN、PPTP 和 L2TP
素质目标	1. 掌握网络安全行业的基本情况 2. 培养良好的职业道德 3. 树立较强的安全意识 4. 培养吃苦耐劳、实事求是、一丝不苟的工作态度 5. 培养分析能力和应变能力

16.4 任务实施

为了完成本工作任务,又细分为以下 3 个子任务。

16.4.1 任务 1:远程访问 VPN 的配置

1. 任务目标

VPN 服务器有两个网络接口,一边连接内部网络;一边连接外部网络。远程或家庭办公用户 A 主机若要与 VPN 服务器通过公网连通,但没有完成 VPN 配置,A 主机不能直接访问总公司内的 B 主机。配置完成后,A 主机能 ping 通 B 主机,说明 VPN 建立成功。

2. 工作任务

(1) 配置 VPN 服务器;

(2) VPN 网络客户端的设置;

(3) VPN 连接检测。

3. 工作环境

两台预装 Windows Server 2003/XP 的主机,通过网络相连,其中一台有两张网卡。

4. 实施过程

(1) 配置 VPN 服务器

① 单击"开始"→"所有程序"→"管理工具",然后选择"路由和远程访问项",进入主窗口。在左边窗格的"路由和远程访问"栏中选中"服务器状态"下的服务器,然后右击,再选择"配置并启用路由和远程访问",如图 16-1 所示。

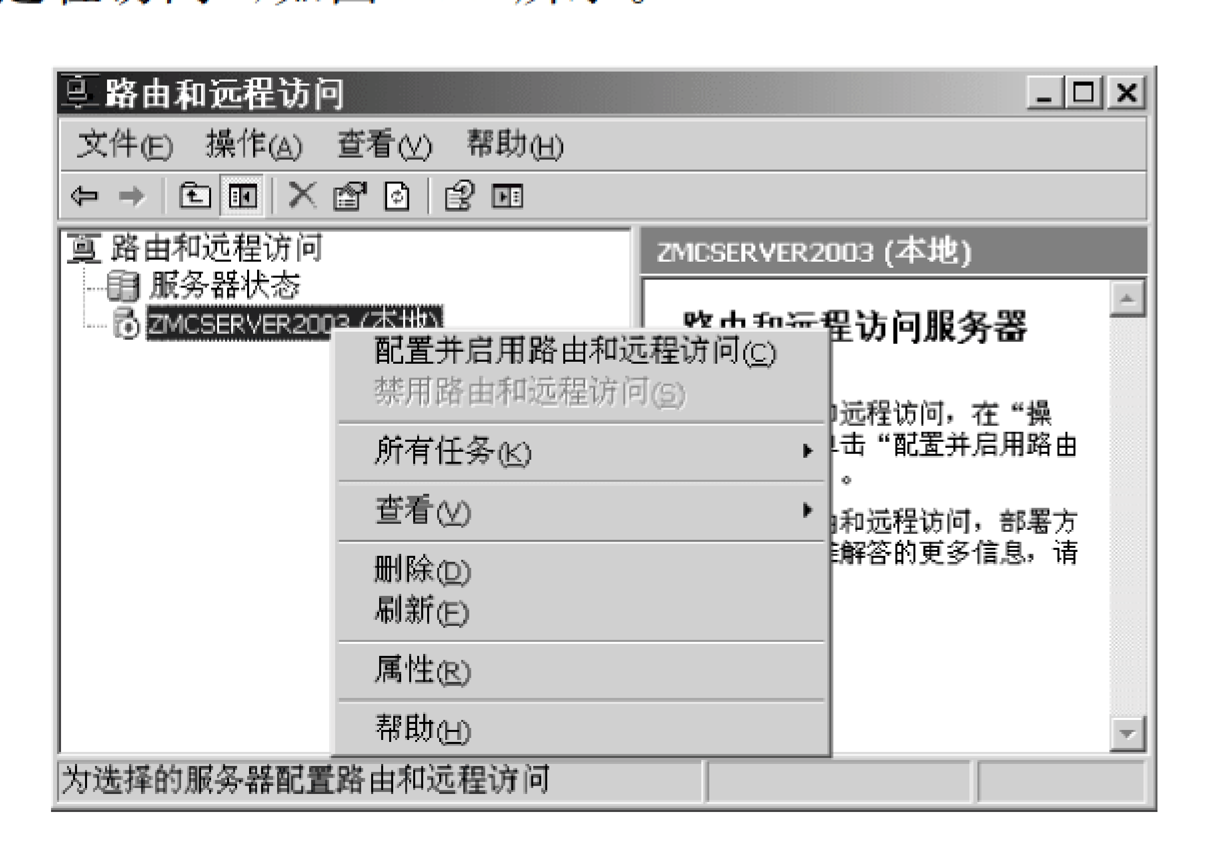


图 16-1 配置并启用路由和远程访问

② 出现提示向导后,单击"下一步"按钮。在配置中选择"虚拟专用网(VPN)访问和 NAT",然后单击"下一步"按钮。

③ 在"VPN 连接"对话框中,选择 VPN 服务器端与外网连接的网卡,如图 16-2 所示。

④ 单击"下一步"按钮,在"IP 地址指定"对话框中,对远程拨入客户指派 IP 地址来源,可以利用 VPN 服务器为连接上来的客户机指定地址范围,如图 16-3 所示。

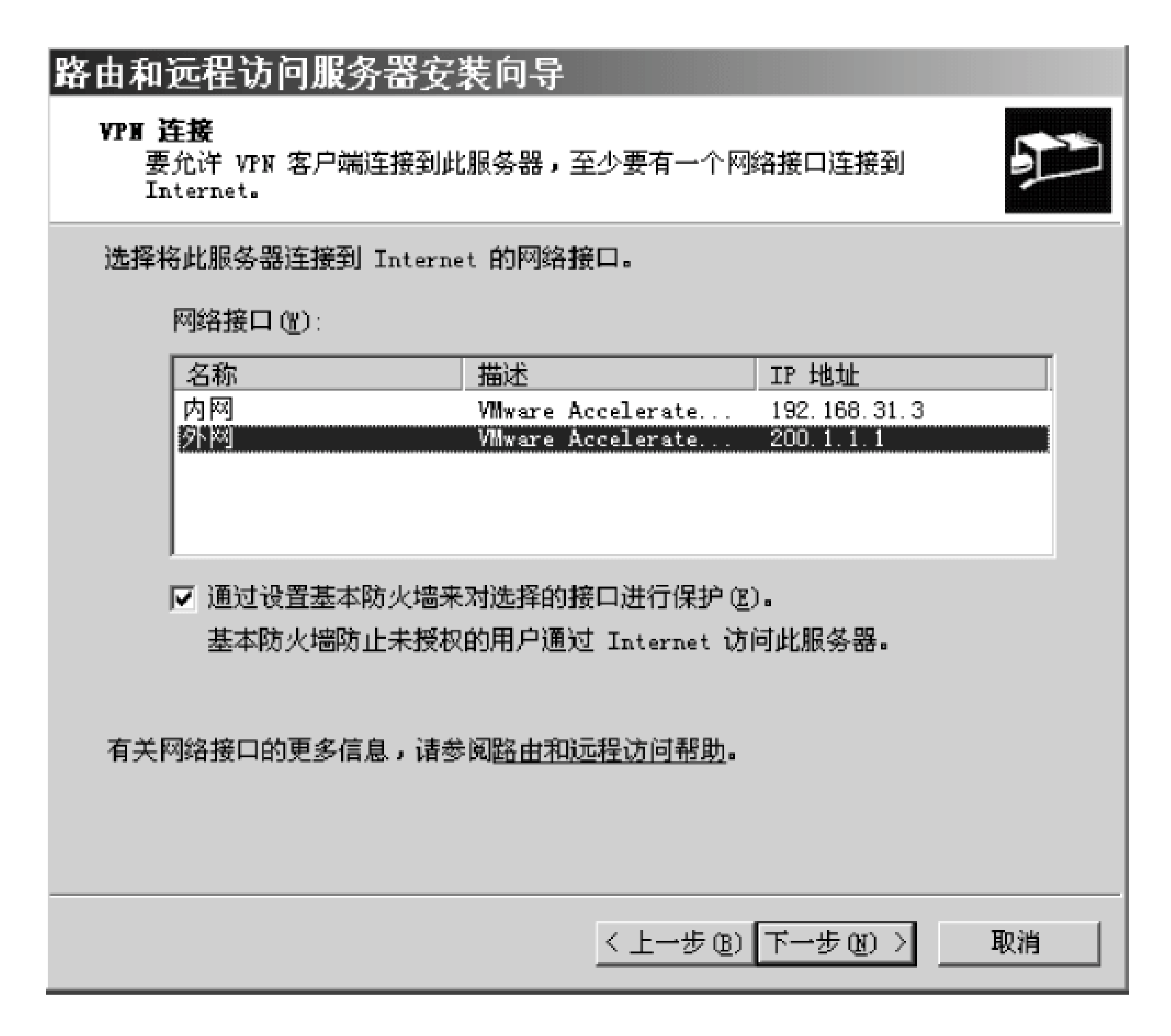


图 16-2　“VPN 连接”对话框

⑤ 单击“下一步”按钮，在“地址范围指定”对话框中单击“新建”按钮。在“新建地址范围”对话框中，输入起始 IP 地址和结束 IP 地址，例如 192.168.31.100 ～192.168.31.109，然后单击“确定”按钮。

⑥ 单击“下一步”按钮，选择不与 RADIUS 一起工作。然后单击“完成”按钮，完成后就可以接收 VPN 客户端的拨入。

⑦ 配置 VPN 服务器中的远程访问策略，允许远程用户在任何时间接入，如图 16-4 所示。

⑧ 新建一个系统用户名、密码均为 vpn-user 的账号，并在用户属性中设置拨入允许 VPN 访问，如图 16-4 所示。

路由和远程访问服务器安装向导
IP 地址指定
您可以选择对远程客户端指派 IP 地址的方法。
您想如何对远程客户端指派 IP 地址?
自动(A)
如果您使用一个 DHCP 服务器指派地址，请确认它配置正确。如果没有使用 DHCP 服务器，此服务器将生成地址。
来自一个指定的地址范围(F)
< 上一步(B) 下一步(N) > 取消

图 16-3　“IP 地址指定”对话框

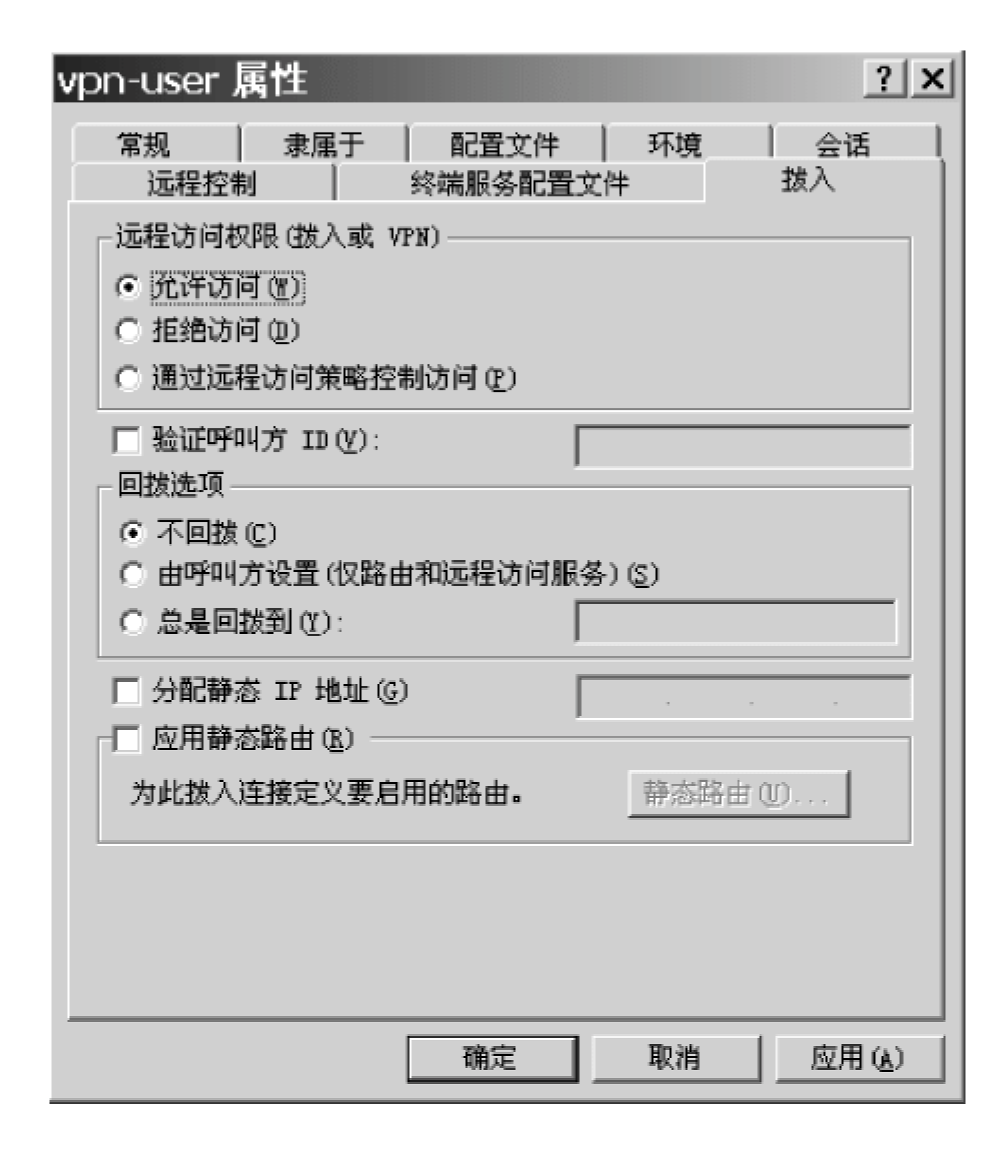


图 16-4　“vpn-user 属性”对话框

（2）VPN 网络客户端的设置

① 新建“网络连接”，然后选择“连接到我的工作场所的网络”选项，如图 16-5 所示。

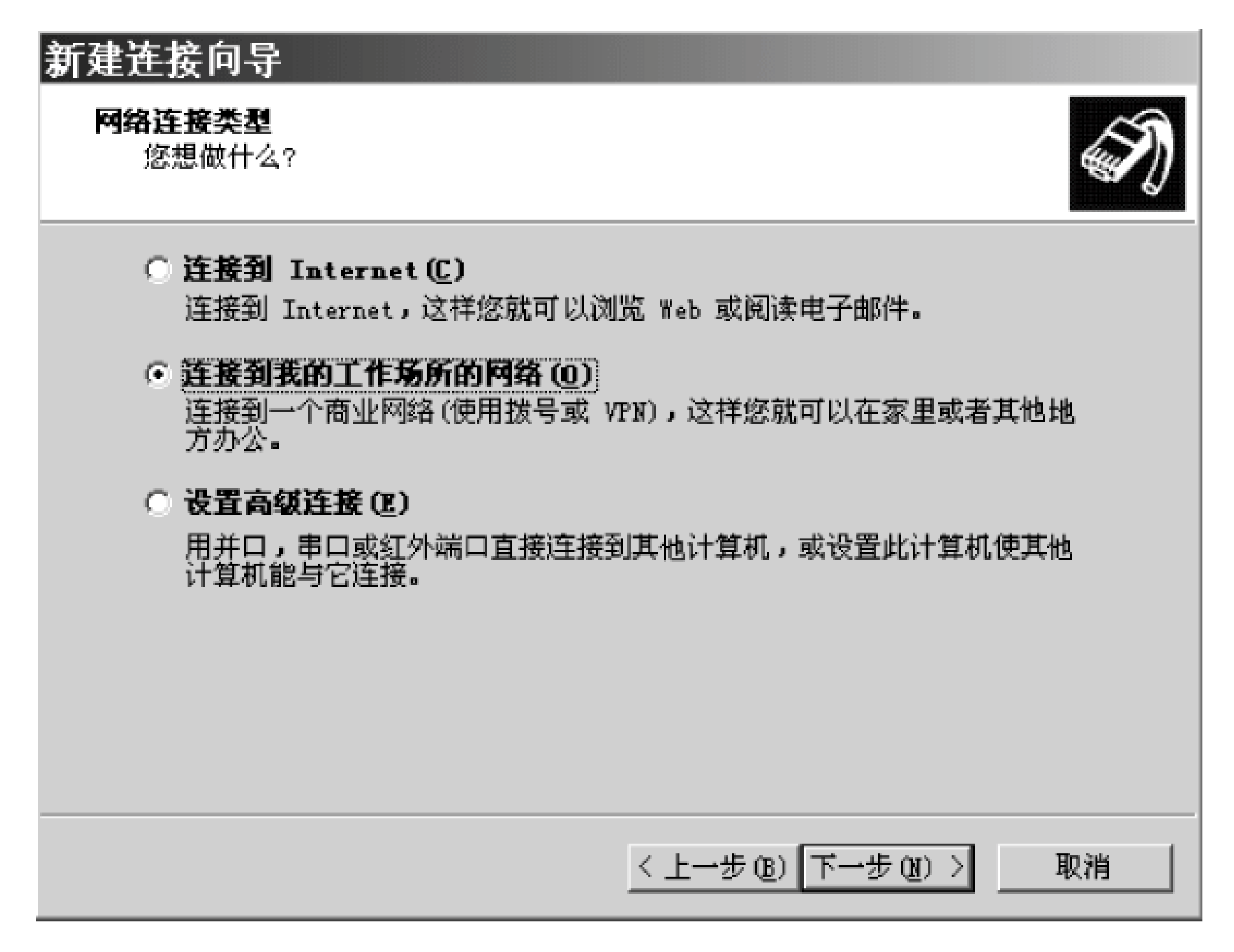


图 16-5 “网络连接类型”对话框

② 单击“下一步”按钮，选择“虚拟专用网络连接”选项，如图 16-6 所示。

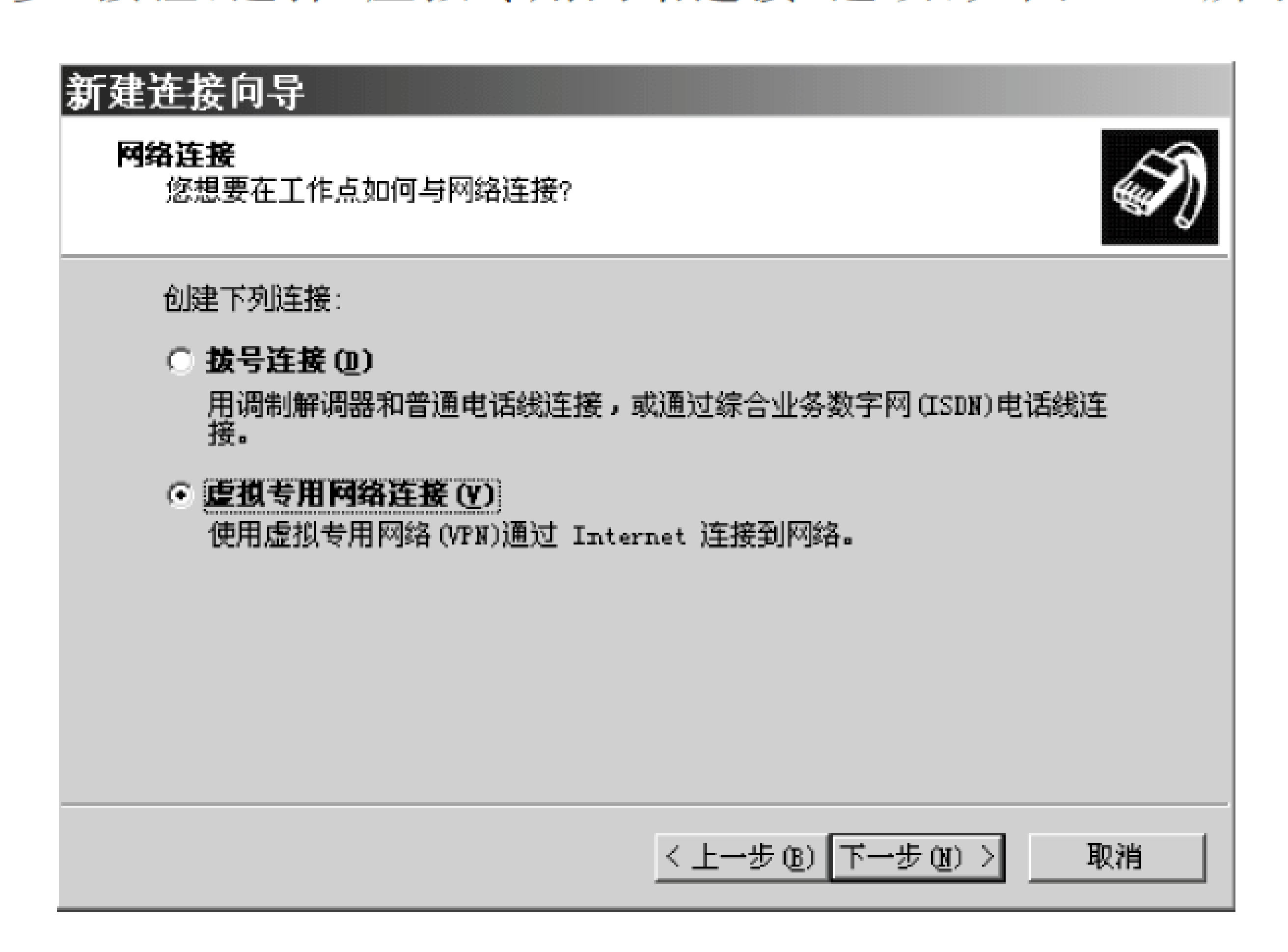


图 16-6 “网络连接”对话框

③ 输入 VPN 服务器的 IP 地址，再按照提示完成 VPN 客户端的设置，如图 16-7 所示。

④ 完成后进行连接，要求输入 VPN 服务器上允许远程拨入的用户名和密码，如图 16-8 所示。

（3）VPN 连接检测

在 VPN 客户端正确连接到 VPN 服务器之后，任务栏会有类似本地连接的 VPN 连接图标出现。

在 VPN 客户机系统中运行 cmd 命令。在命令行窗口执行 ipconfig，可以查看到客户机已经获取的新地址与内部网络在同一个网段内了，如图 16-9 所示。此时，在客户机上 ping 内网段 IP，已经可以 ping 通。

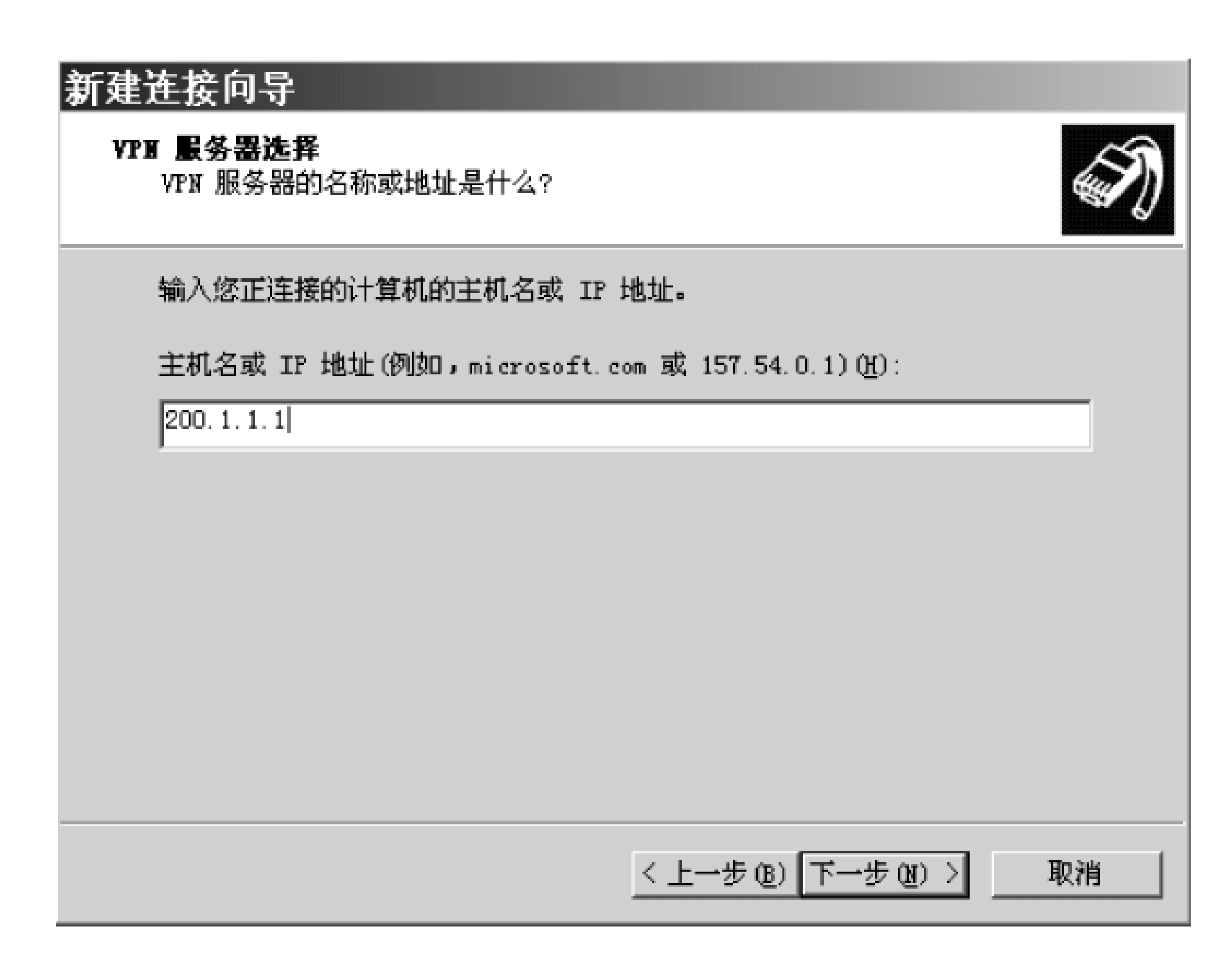


图 16-7　“VPN 服务器选择”对话框



图 16-8　连接 VPN 服务器对话框



图 16-9　VPN 连接检测

16.4.2　任务 2：点对点通信 VPN 连接的配置

1. 任务目标

为了实现企业内部网的两台主机之间安全通信，即单机到单机结构中都采用 Windows 系统时的 VPN 连接，配置主机 A 和主机 B 之间的数据采用安全的 VPN 进行连接（IPSec 的 VPN）。

2. 工作任务

（1）创建 IPSec 策略；

（2）建立从 A 到 B 的筛选器列表；

（3）建立从 B 到 A 的筛选器列表；

（4）为 A 到 B 隧道配置规则；

（5）为 B 到 A 隧道配置规则；

（6）将新的 IPSec 策略指派。

3. 工作环境

两台预装 Windows Server 2003/XP 的主机，通过网络相连。

4. 实施过程

假定两台预装 Windows Server 2003/XP 的主机 A 和 B 处于同一局域网中，即同一网段，A 的 IP 地址是 192.168.31.3，B 的 IP 地址是 192.168.31.111。配置实现 A 和 B 安全的 ICMP 通信，对 ICMP 协议进行 VPN 加密传输。具体的操作步骤如下所示。

（1）创建 IPSec 策略

① 单击“开始”→“运行”，然后输入“secpol.msc”启动“本地安全设置”。

② 右击“IP 安全策略，在本地计算机”，在弹出的快捷菜单中选择“创建 IP 安全策略”。

③ 单击“下一步”按钮，然后输入策略名称“IPSec 策略”，再单击“下一步”按钮。

④ 撤选“激活默认响应规则”复选框，然后单击“下一步”按钮。

⑤ 保持“编辑属性”复选框选中状态，单击“完成”按钮。

（2）建立从 A 到 B 的筛选器列表

① 弹出“IPSec 策略 属性”对话框，撤选窗口右下角“使用‘添加’向导”复选框，然后单击“添加”按钮，创建新 IP 安全规则，如图 16-10 所示。

② 弹出“新规则 属性”对话框，选择“IP 筛选器列表”选项卡，然后单击“添加”按钮，如图 16-11 所示。



图 16-10 “规则”选项卡(1)

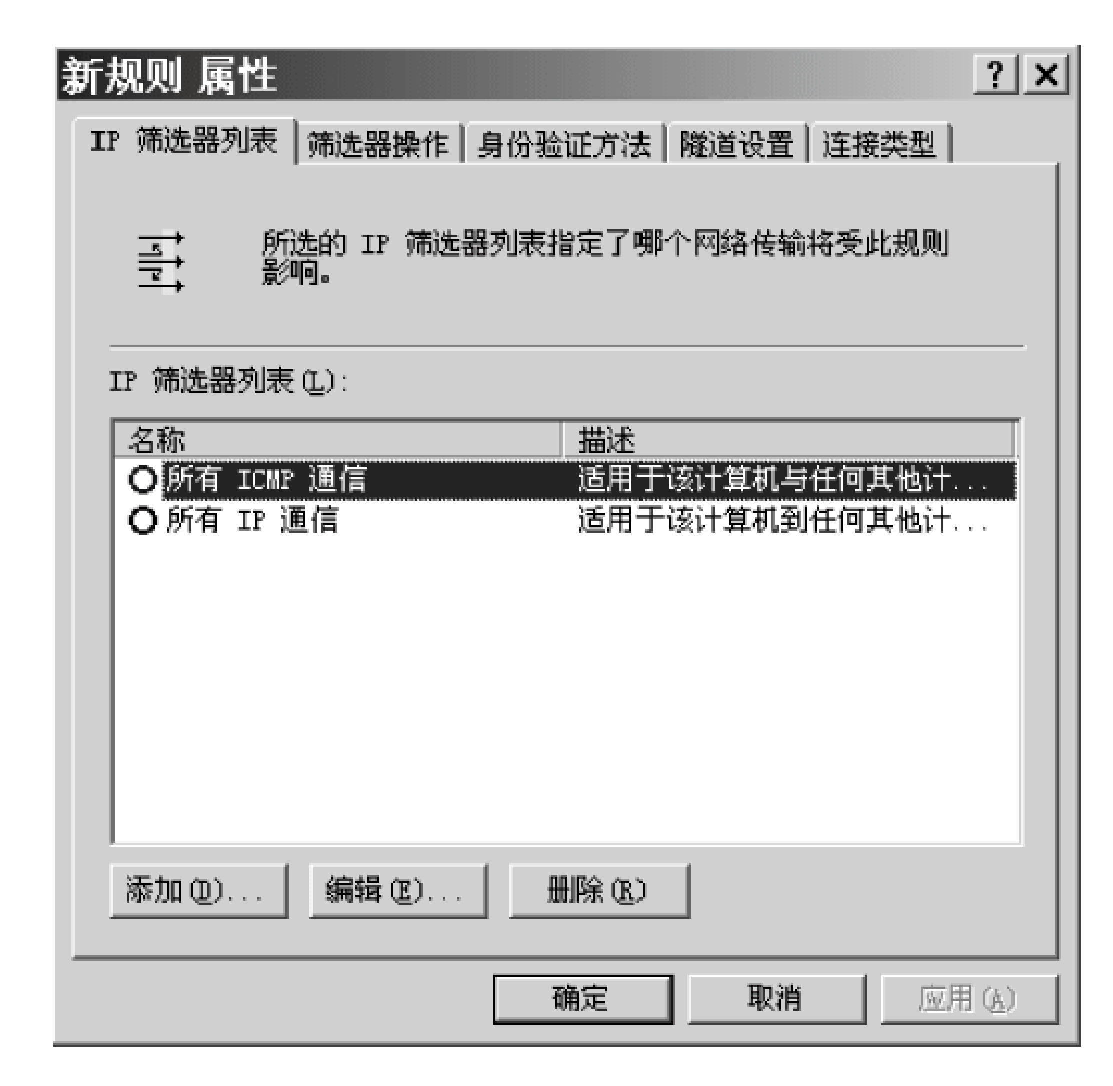


图 16-11 “IP 筛选器列表”选项卡(1)

③ 弹出“IP 筛选器列表”对话框，在名称文本框输入新 IP 筛选器列表名称“A 到 B 筛选器列表”，再撤选右侧“使用添加向导”复选框，然后单击“添加”按钮，如图 16-12 所示。

④ 弹出“IP 筛选器 属性”对话框，选择“地址”选项卡。在“源地址”下拉列表框中，选择“一个特定的 IP 地址”，输入 A 的 IP 地址“192.168.31.3”；在“目的地址”下拉列表框中，选择“一个特定的 IP 地址”，输入 B 的 IP 地址“192.168.31.111”，并撤选“镜像”复选框，如图 16-13 所示。

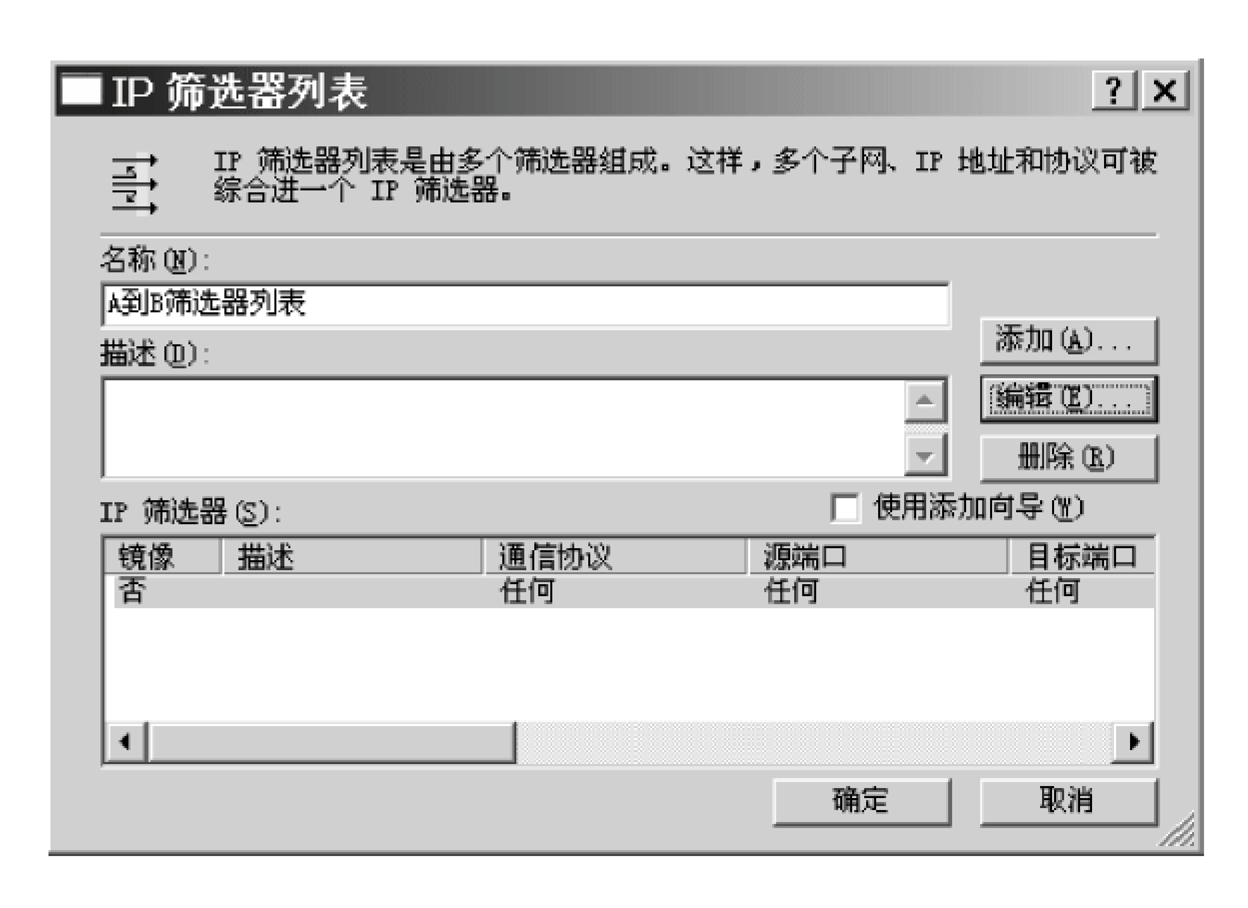


图 16-12　“IP 筛选器列表”对话框(1)

⑤ 选择“协议”选项卡，将协议类型设置为“任意”，因为 IPSec 隧道不支持协议或端口特定的筛选器。

⑥ 选择“描述”选项卡，可以为 IP 筛选器指定一个名称或简短描述，然后单击“确定”按钮。

(3) 建立从 B 到 A 的筛选器列表

① 返回“新规则 属性”对话框，选择“IP 筛选器列表”选项卡，然后单击“添加”按钮，如图 16-14 所示。

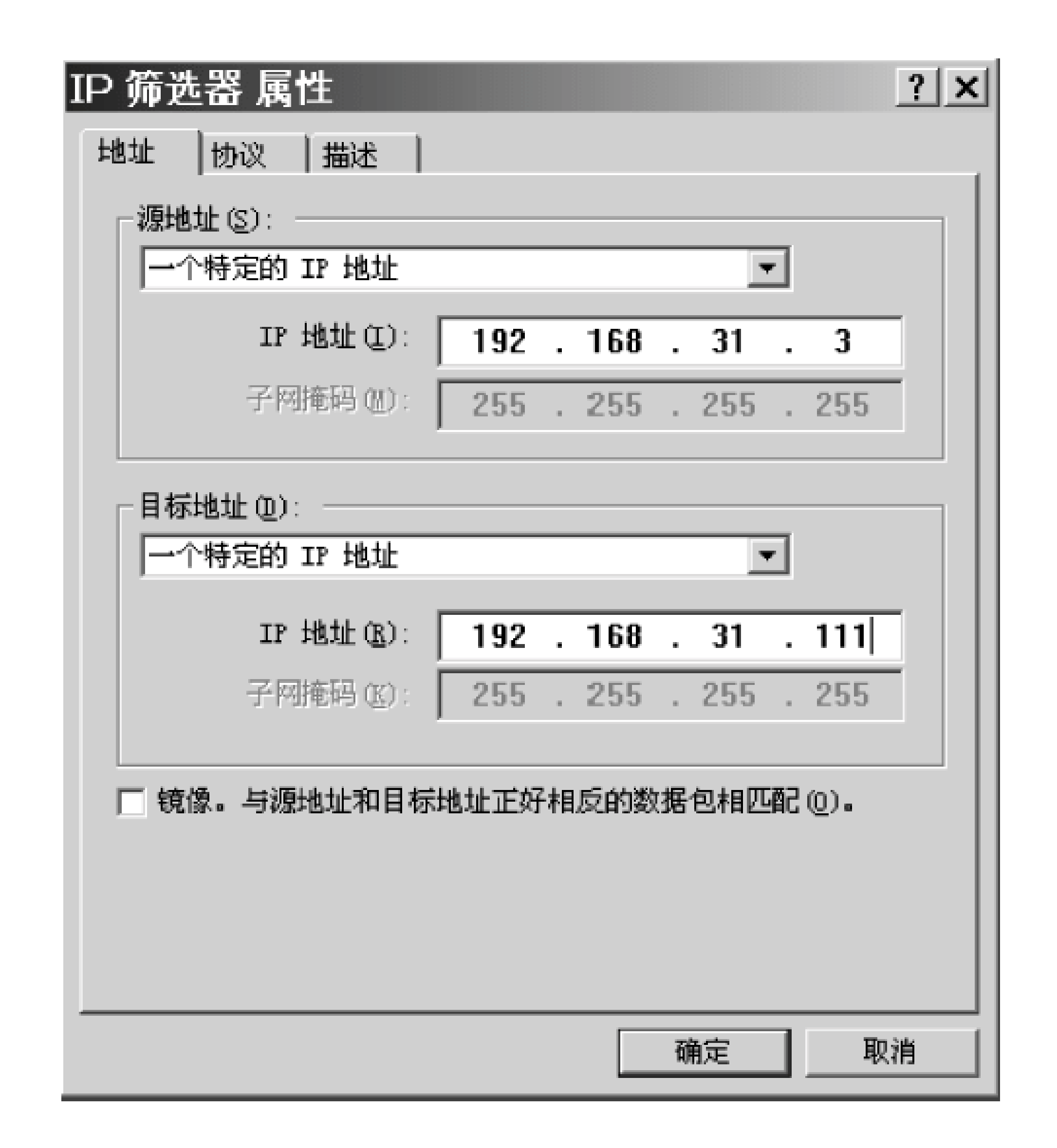


图 16-13　“地址”选项卡(1)

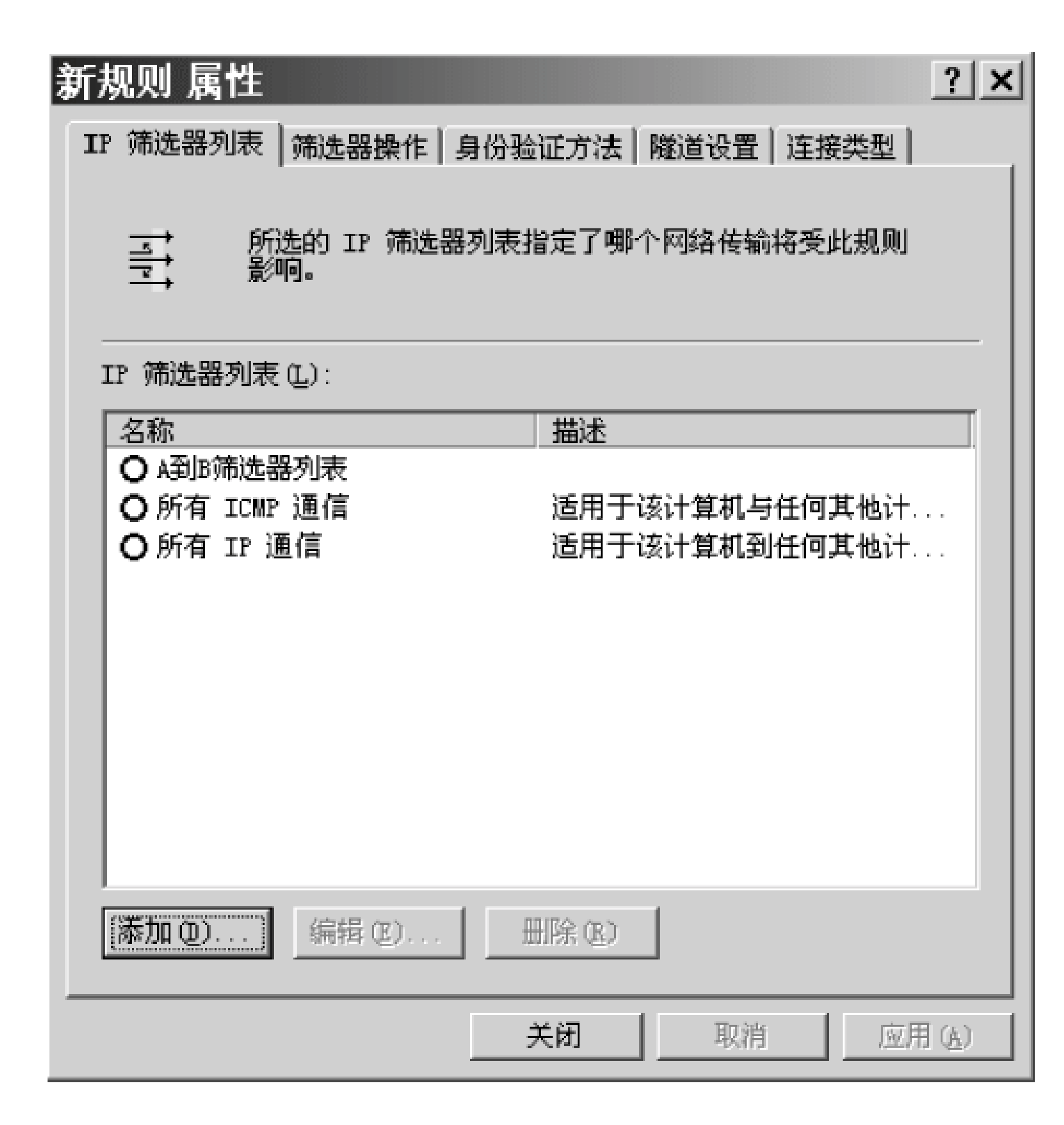


图 16-14　“IP 筛选器列表”选项卡(2)

② 弹出“IP 筛选器列表”对话框，在名称文本框输入新 IP 筛选器列表名称“B 到 A 筛选器列表”，再撤选右侧“使用添加向导”复选框，然后单击“添加”按钮，如图 16-15 所示。

③ 弹出“IP 筛选器 属性”对话框，选择“地址”选项卡。在“源地址”下拉列表框中，选择“一个特定的 IP 地址”，输入 B 的 IP 地址“192.168.31.111”；在“目的地址”下拉列表框中，

选择“一个特定的 IP 地址”，输入 A 的 IP 地址“192.168.31.3”，并撤选“镜像”复选框，如图 16-16 所示。

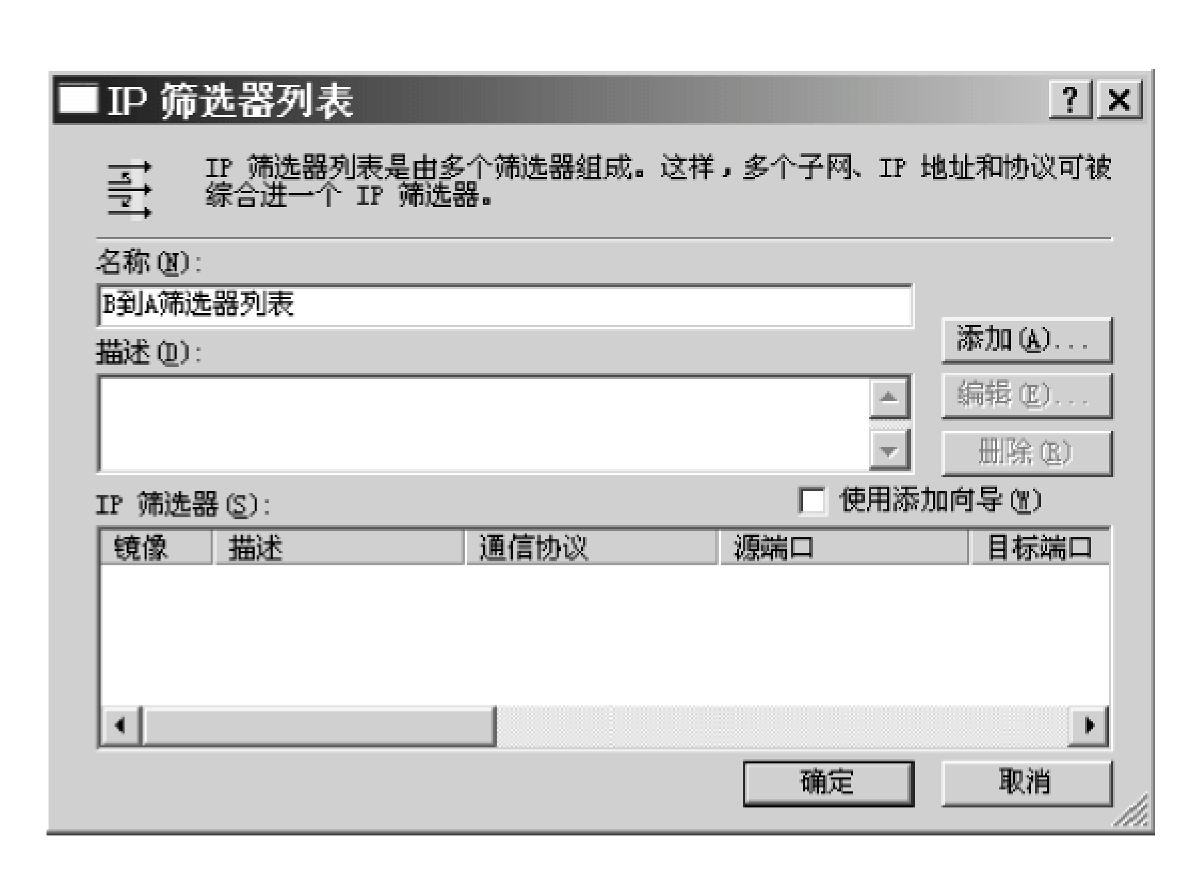


图 16-15 “IP 筛选器列表”对话框(2)

IP 筛选器 属性
地址 | 协议 | 描述
源地址(S):
一个特定的 IP 地址
IP 地址(I): 192 . 168 . 31 . 111
子网掩码(M): 255 . 255 . 255 . 255
目标地址(D):
一个特定的 IP 地址
IP 地址(R): 192 . 168 . 31 . 3
子网掩码(K): 255 . 255 . 255 . 255
镜像。与源地址和目标地址正好相反的数据包相匹配(O)。
确定 取消

图 16-16 “地址”选项卡(2)

④ 选择“协议”选项卡，将协议类型设置为“任意”，因为 IPSec 隧道不支持协议或端口特定的筛选器。

⑤ 选择“描述”选项卡，为 IP 筛选器指定一个名称或简短描述，然后单击“确定”按钮。

⑥ 单击“确定”按钮。

(4) 为 A 到 B 隧道配置规则

① 返回“新规则 属性”对话框，选择“IP 筛选器列表”选项卡，然后选中“A 到 B 筛选器列表”，如图 16-17 所示。

② 单击“隧道设置”选项卡，单击“隧道终点由此 IP 地址指定”框，然后输入 IP，这是分配给非 Microsoft 网关外部网络适配器的 IP 地址，如图 16-18 所示。

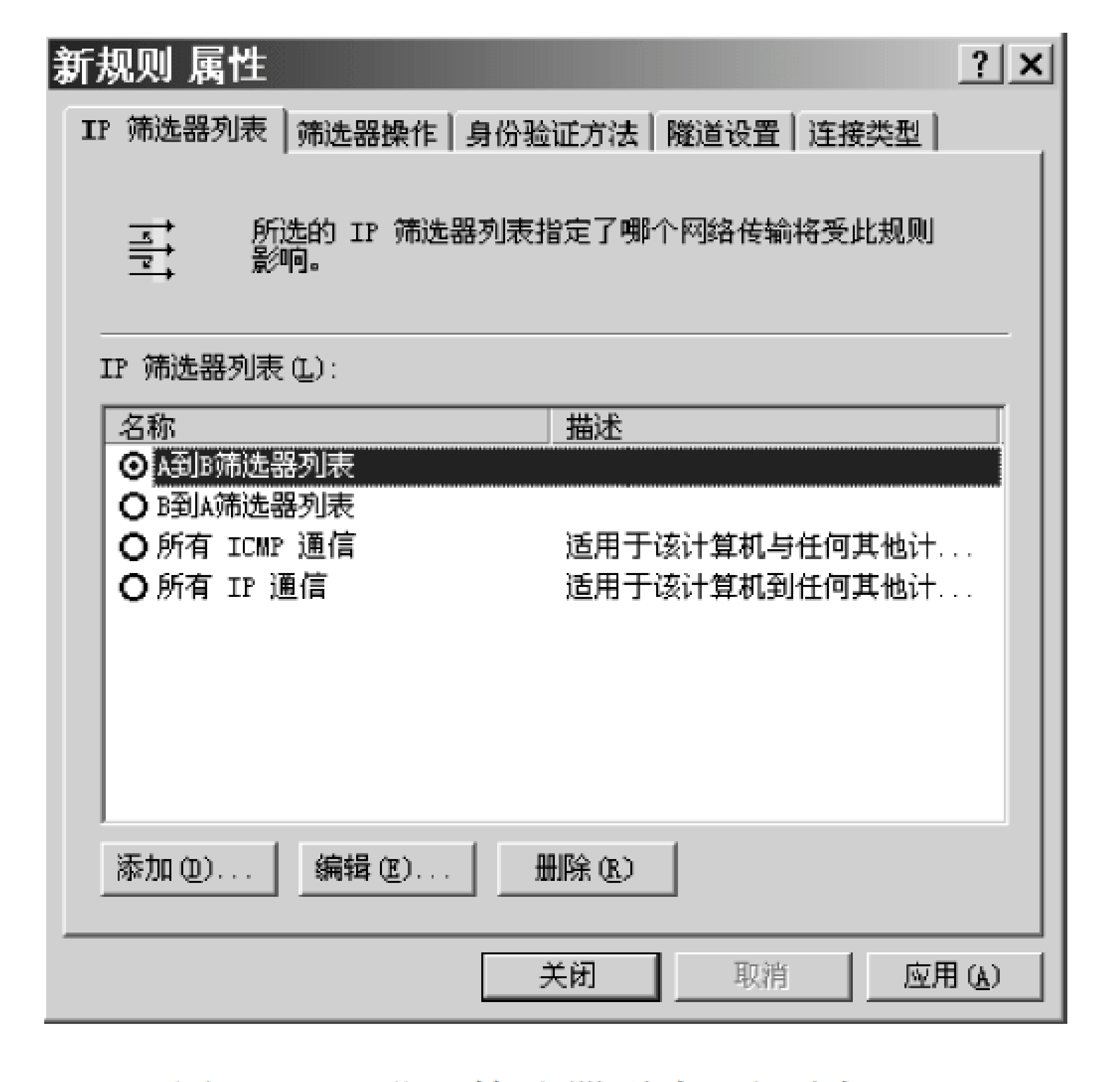


图 16-17 “IP 筛选器列表”选项卡(3)

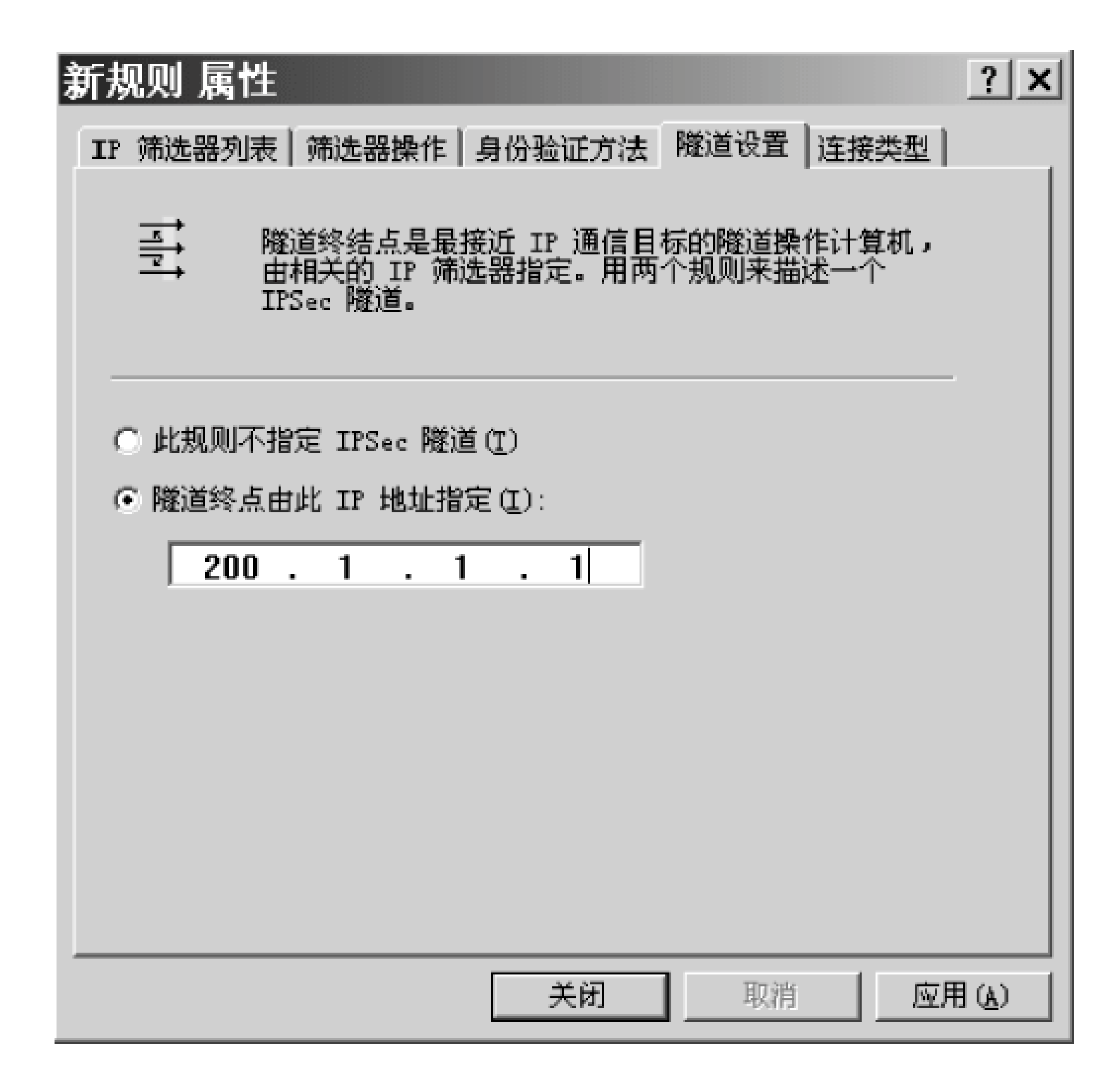


图 16-18 “隧道设置”选项卡(1)

③ 单击“连接类型”选项卡，选择“所有网络连接”。注意，如果不是 ISDN、PPP 或直连串行连接，则单击“局域网(LAN)”。

④ 单击“筛选器操作”选项卡，撤选右下角“使用添加向导”复选框，然后单击“添加”按钮，以创建新的筛选器操作，如图 16-19 所示。

⑤ 在“新筛选器操作 属性”对话框的“安全措施”选项卡中，保持“协商安全”选项为启用状态，并撤选“接受不安全的通信，但总是用 IPSec 响应”复选框，然后单击“添加”按钮，如图 16-20 所示。

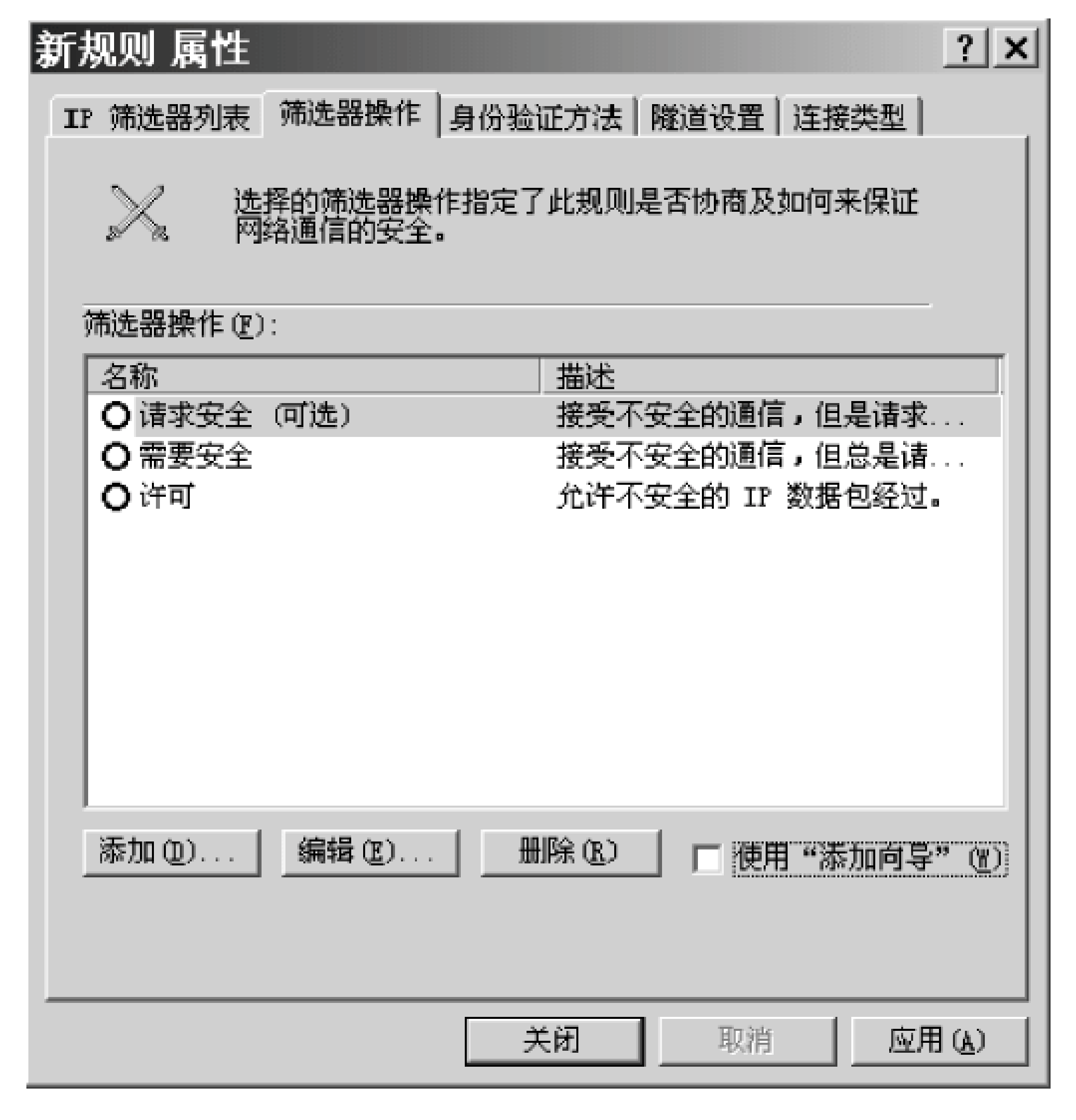


图 16-19　“筛选器操作”选项卡(1)

图 16-20　“安全措施”选项卡(1)

⑥ 保持“完整性和加密”选项为选中状态，单击“确定”按钮，如图 16-21 所示。

⑦ 单击“常规”选项卡，输入新筛选器操作的名称“A 到 B 隧道规则”，并单击“确定”按钮，如图 16-22 所示。

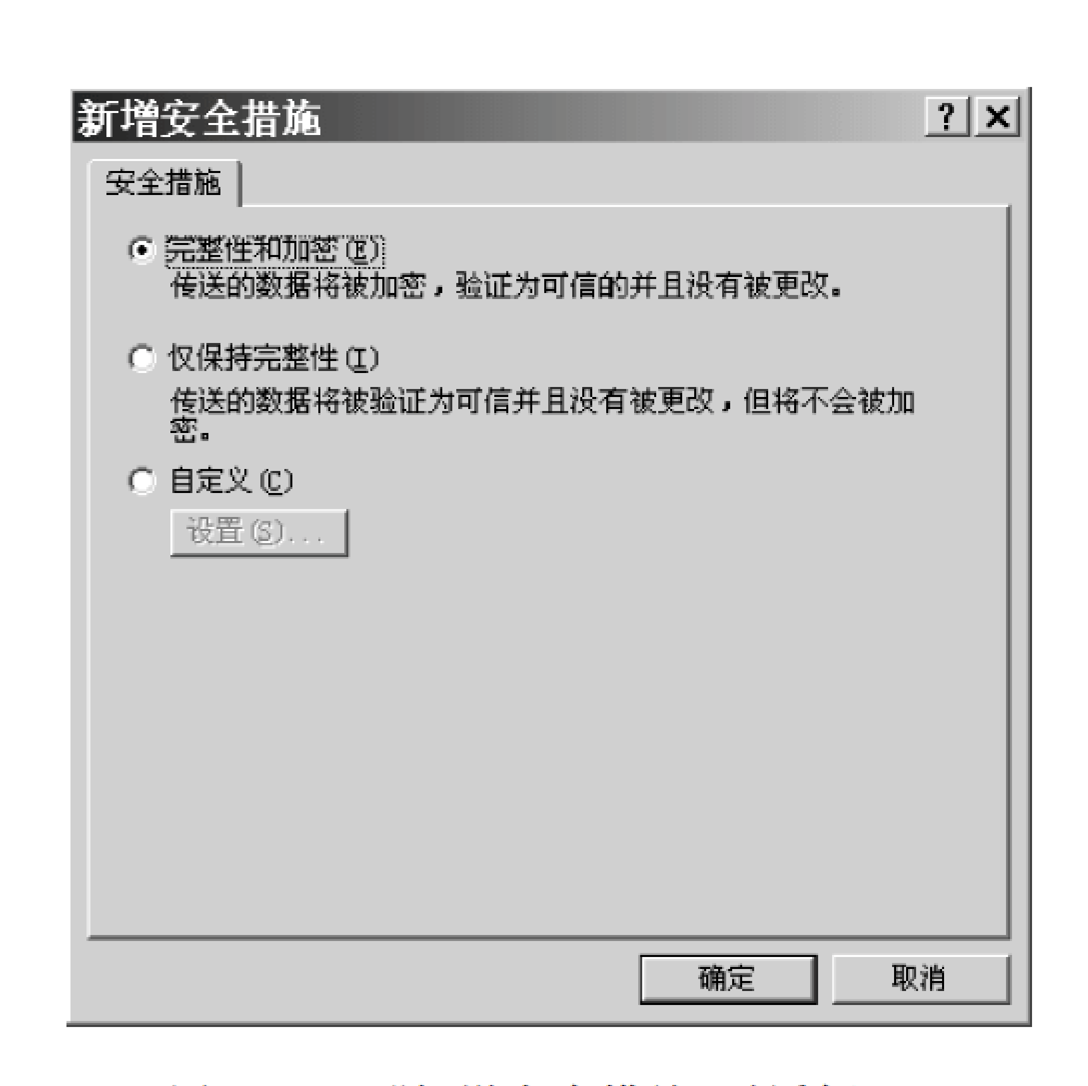


图 16-21　“新增安全措施”对话框(1)

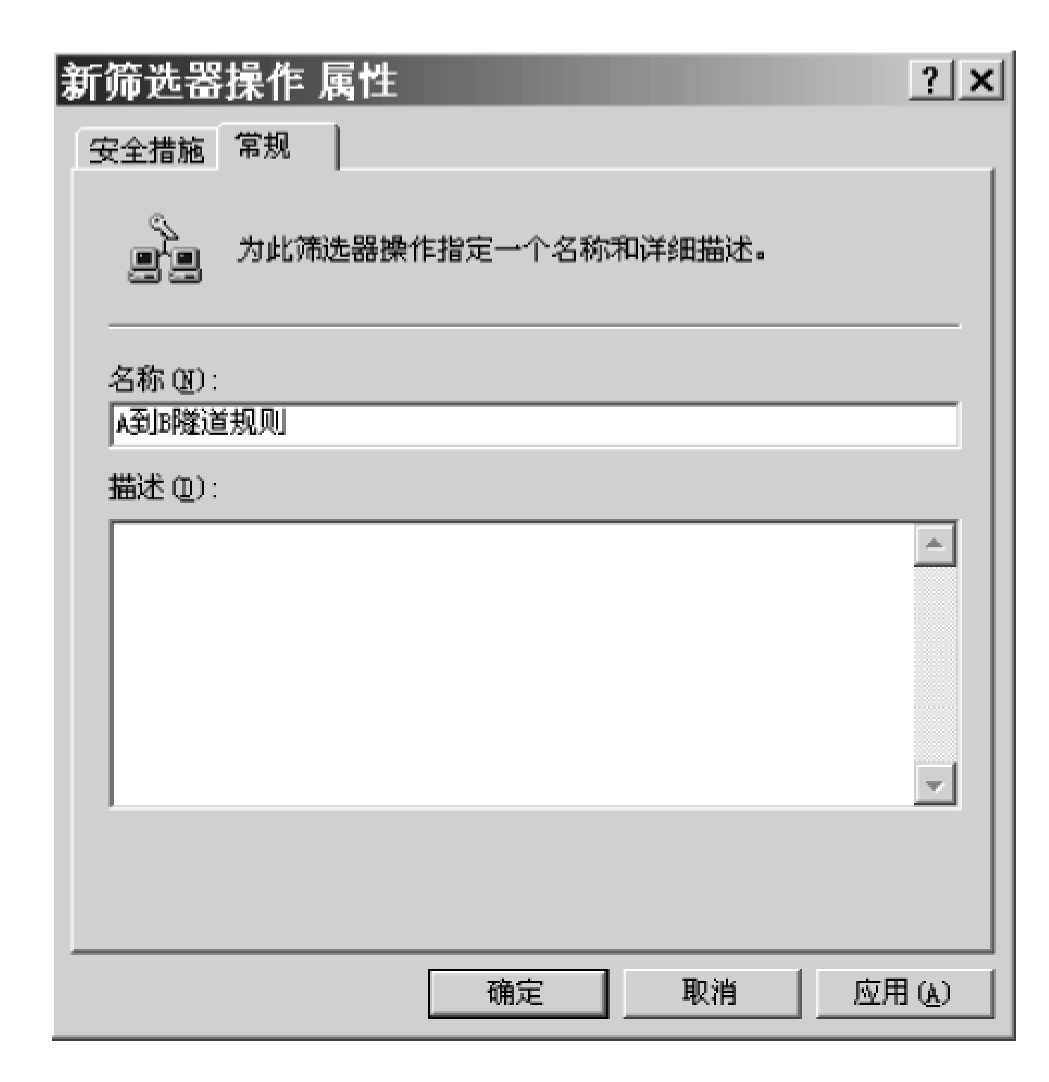


图 16-22　“常规”选项卡

⑧ 单击刚创建的筛选器操作“A 到 B 隧道规则”，将其选中，如图 16-23 所示。

⑨ 单击“身份验证方法”选项卡，配置所需的身份验证方法。如果为了测试，使用“预共享密钥”，否则使用“证书”。如果隧道的两个终结点都在受信任域中，并且在隧道的 IKE 协商期间（在建立隧道前），隧道的两个终结点都可以访问网络上每个受信任域的 IP 地址，从技术上说 Kerberos 是可行的，不过这种情况很少见。

⑩ 单击“关闭”按钮。

（5）为 B 到 A 隧道配置规则

① 在“IPSec 策略 属性”对话框中，单击“添加”按钮，以创建新规则，如图 16-24 所示。

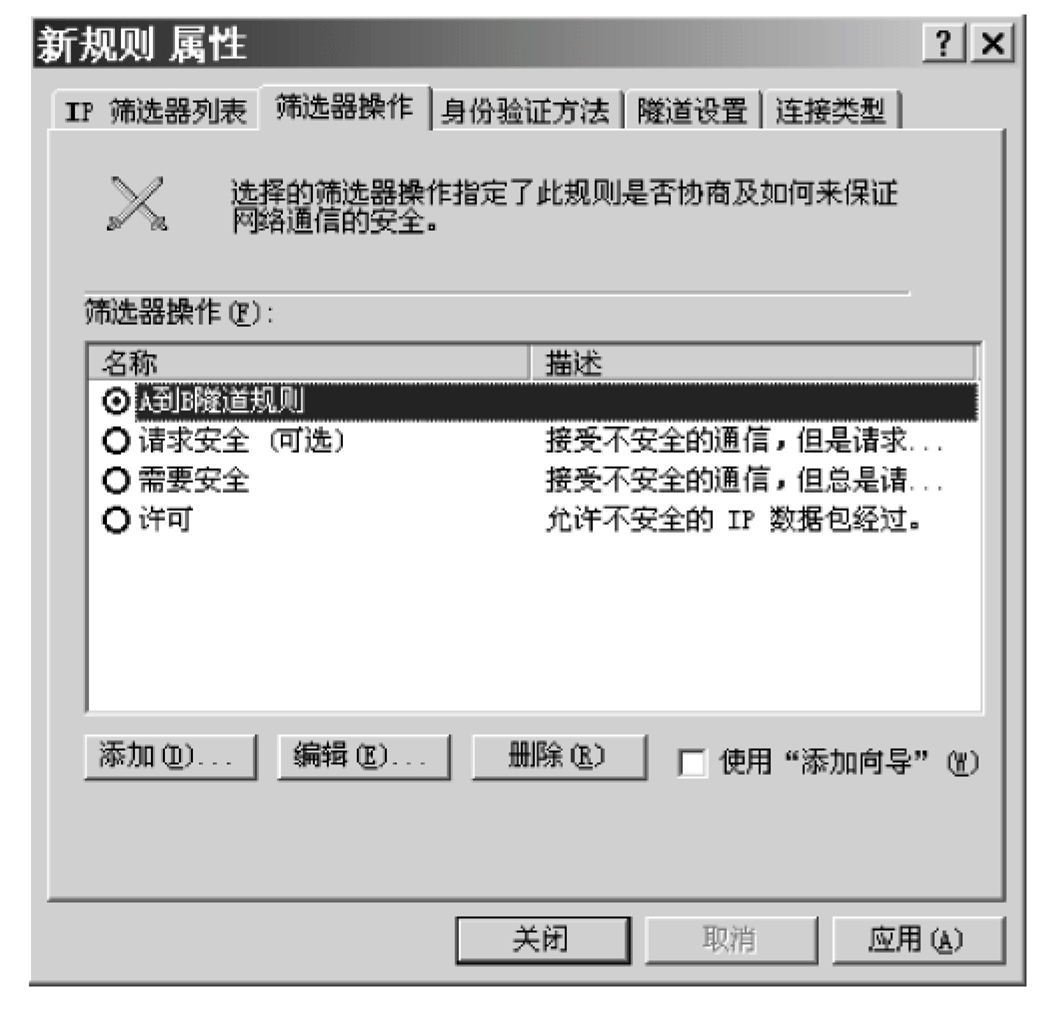


图 16-23　“筛选器操作”选项卡(2)



图 16-24　“规则”选项卡(2)

② 弹出“新规则 属性”对话框，选择“IP 筛选器列表”选项卡，然后单击创建的“B 到 A 筛选器”列表，将其选中，如图 16-25 所示。

③ 单击“隧道设置”选项卡，再单击“隧道终点由此 IP 地址指定”框，然后输入 IP 地址，这是分配给非 Microsoft 网关外部网络适配器的 IP 地址，如图 16-26 所示。

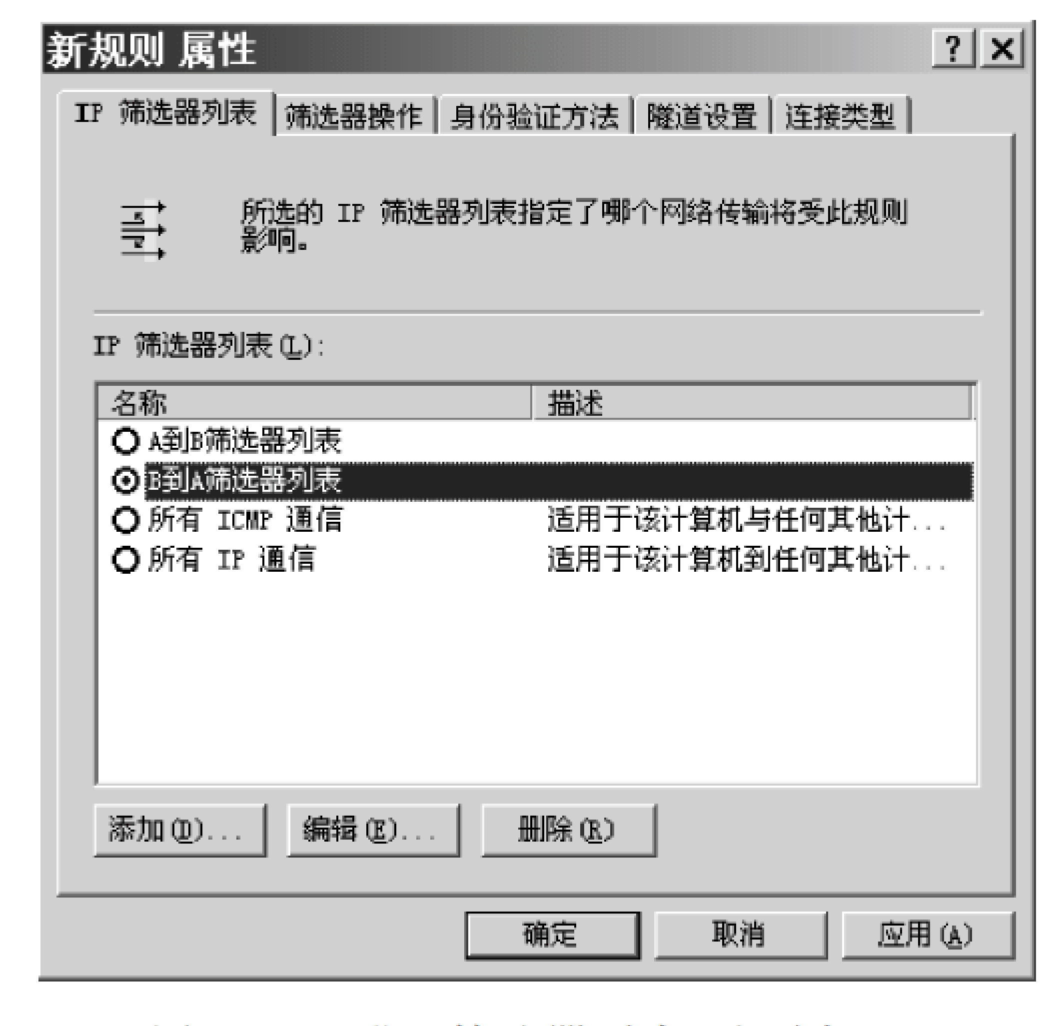


图 16-25　“IP 筛选器列表”选项卡(4)

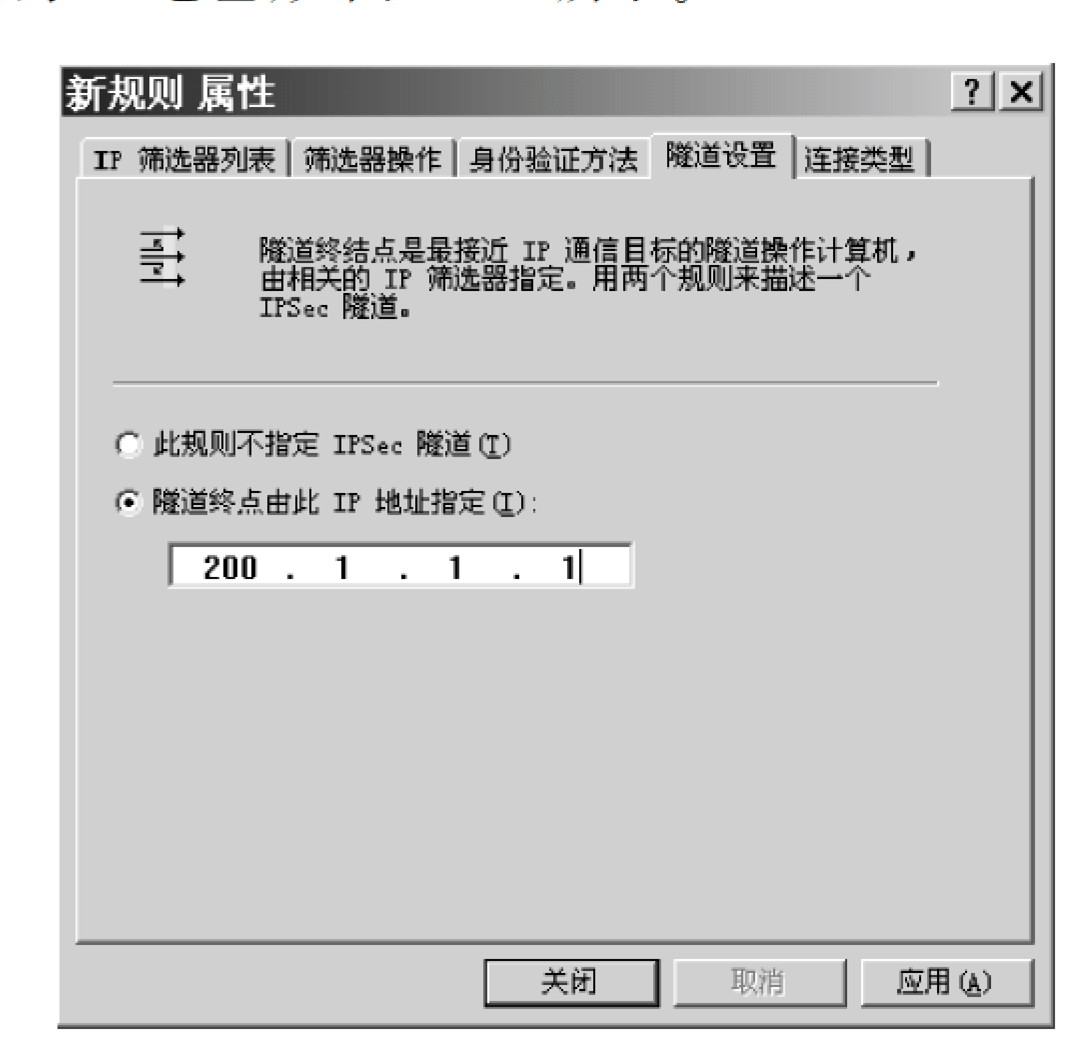


图 16-26　“隧道设置”选项卡(2)

④ 选择“连接类型”选项卡，再单击“所有网络连接”。注意，如果不是ISDN、PPP或直连串行连接，则单击“局域网(LAN)”。与筛选器匹配的接口类型上的所有出站通信流都将尝试通过隧道传输到在规则中指定的隧道终结点。与筛选器匹配的入站通信流将被丢弃，因为它的接收应受到IPSec隧道的安全保护。

⑤ 单击“筛选器操作”选项卡，撤选右下角“使用添加向导”复选框，然后单击“添加”按钮，以创建新的筛选器操作，如图16-27所示。

⑥ 在“新筛选器操作 属性”对话框的“安全措施”选项卡中，保持“协商安全”选项为启用状态，再撤选“接受不安全的通信，但总是用IPSec响应”复选框，然后单击“添加”按钮，如图16-28所示。

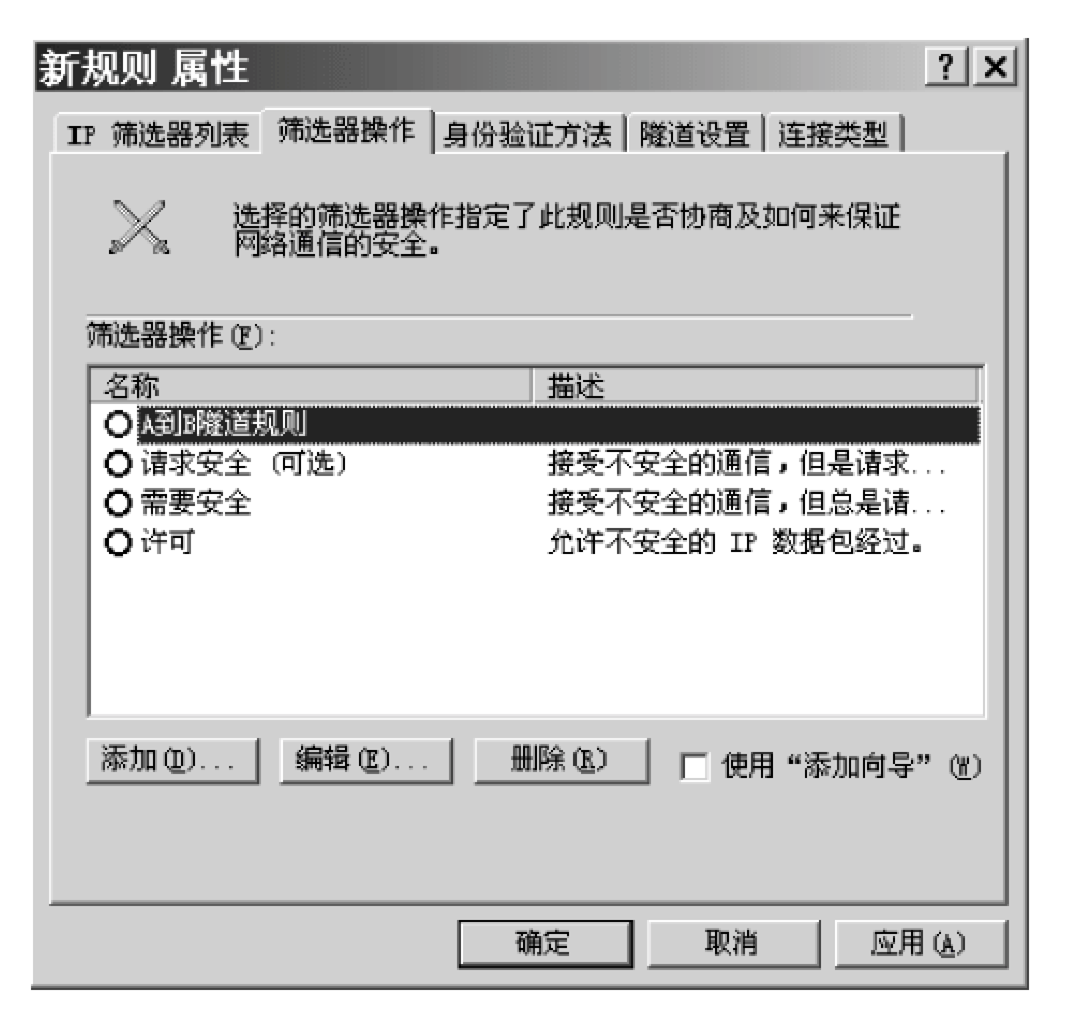


图16-27　“筛选器操作”选项卡(3)

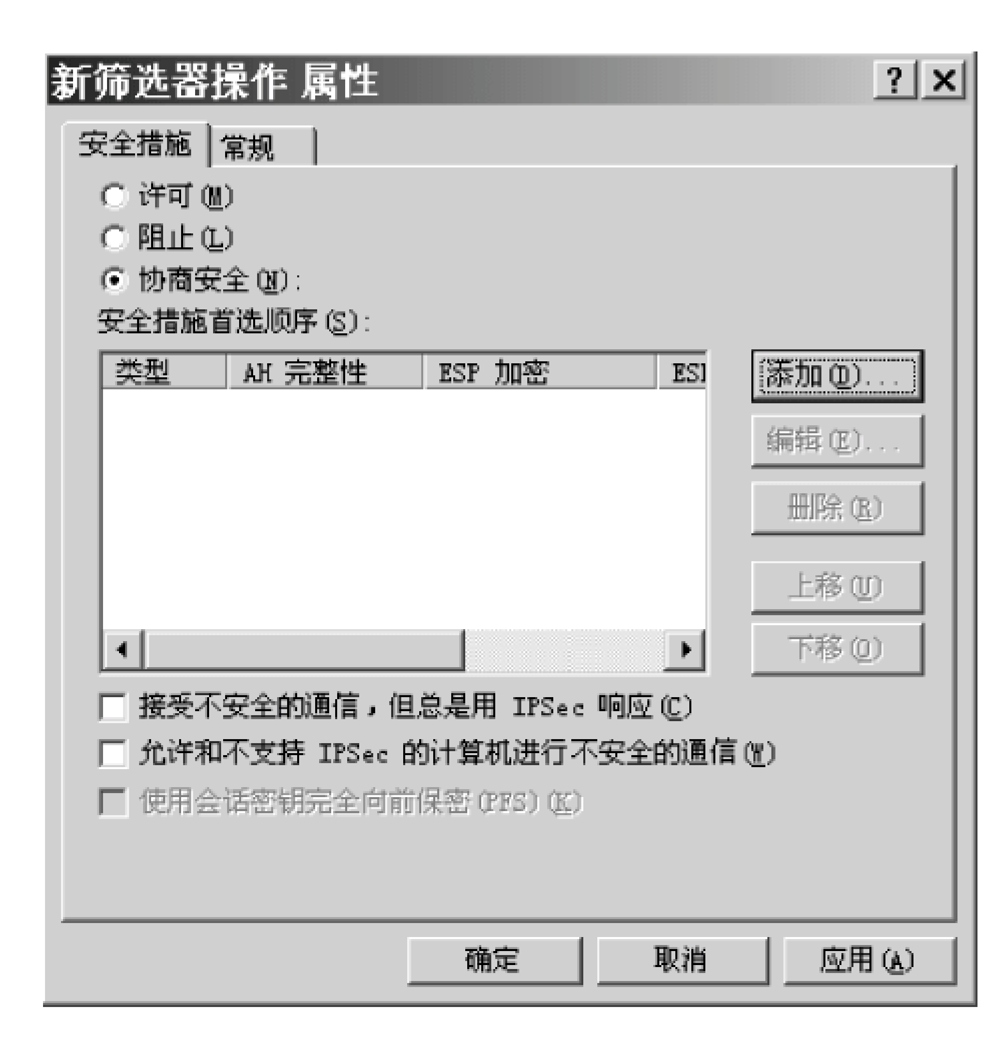


图16-28　“安全措施”选项卡(2)

⑦ 保持“完整性和加密”选项为选中状态，然后单击“确定”按钮，如图16-29所示。

⑧ 单击“常规”选项卡，输入新筛选器操作的名称“B到A隧道规则”，并单击“确定”按钮。

⑨ 单击刚创建的筛选器操作“B到A隧道规则”，将其选中，如图16-30所示。

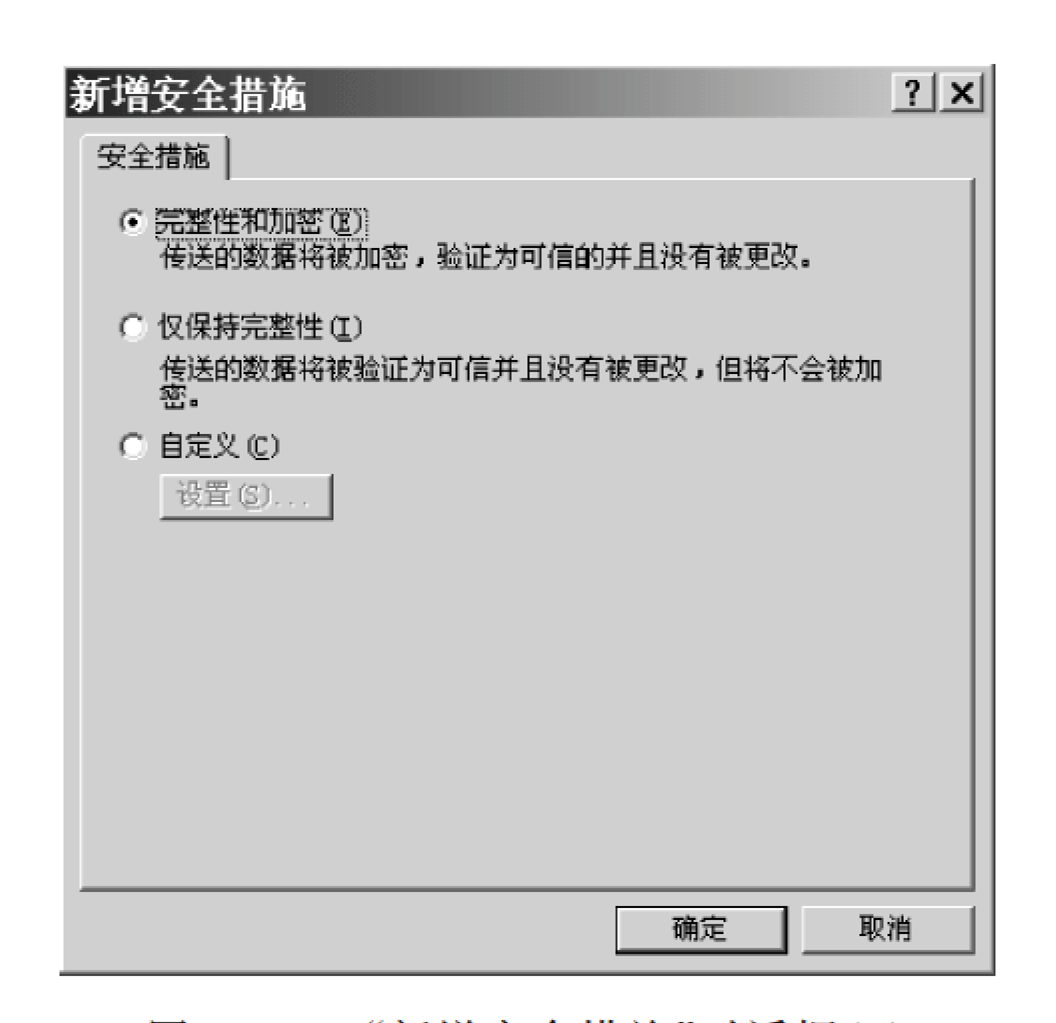


图16-29　“新增安全措施”对话框(2)

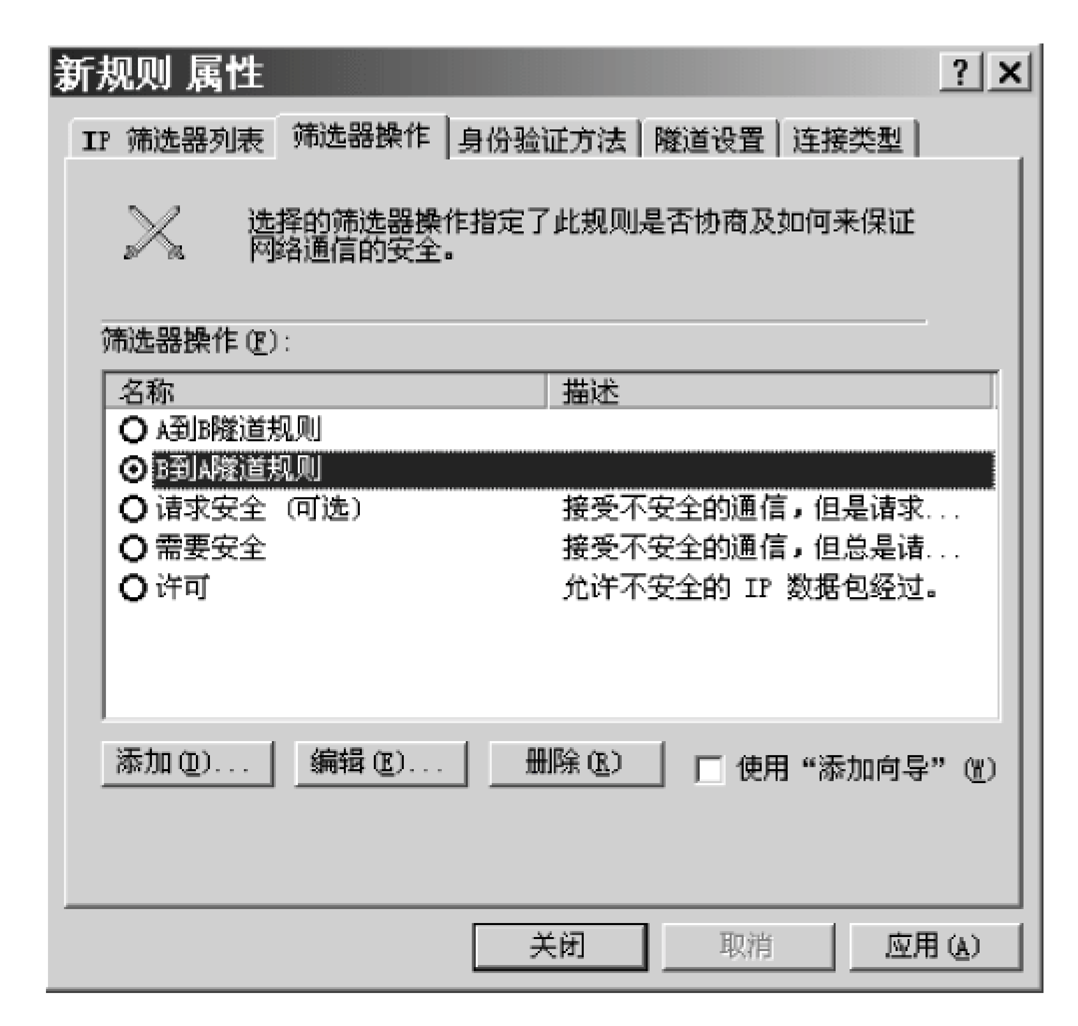


图16-30　“筛选器操作”选项卡(4)

⑩ 选择“身份验证方法”选项卡，配置在第一个规则中使用的同一种方法。

⑪ 单击“确定”按钮，确保创建的这两个规则在策略中都已经启用，然后再次单击“确定”按钮。

(6) 将新的 IPSec 策略指派

在本地计算机 MMC 管理单元上的“IP 安全策略”中，右击“新策略”，然后单击“指定”。该策略旁边的文件夹图标中将出现一个绿色箭头，表示已经启用，如图 16-31 所示。

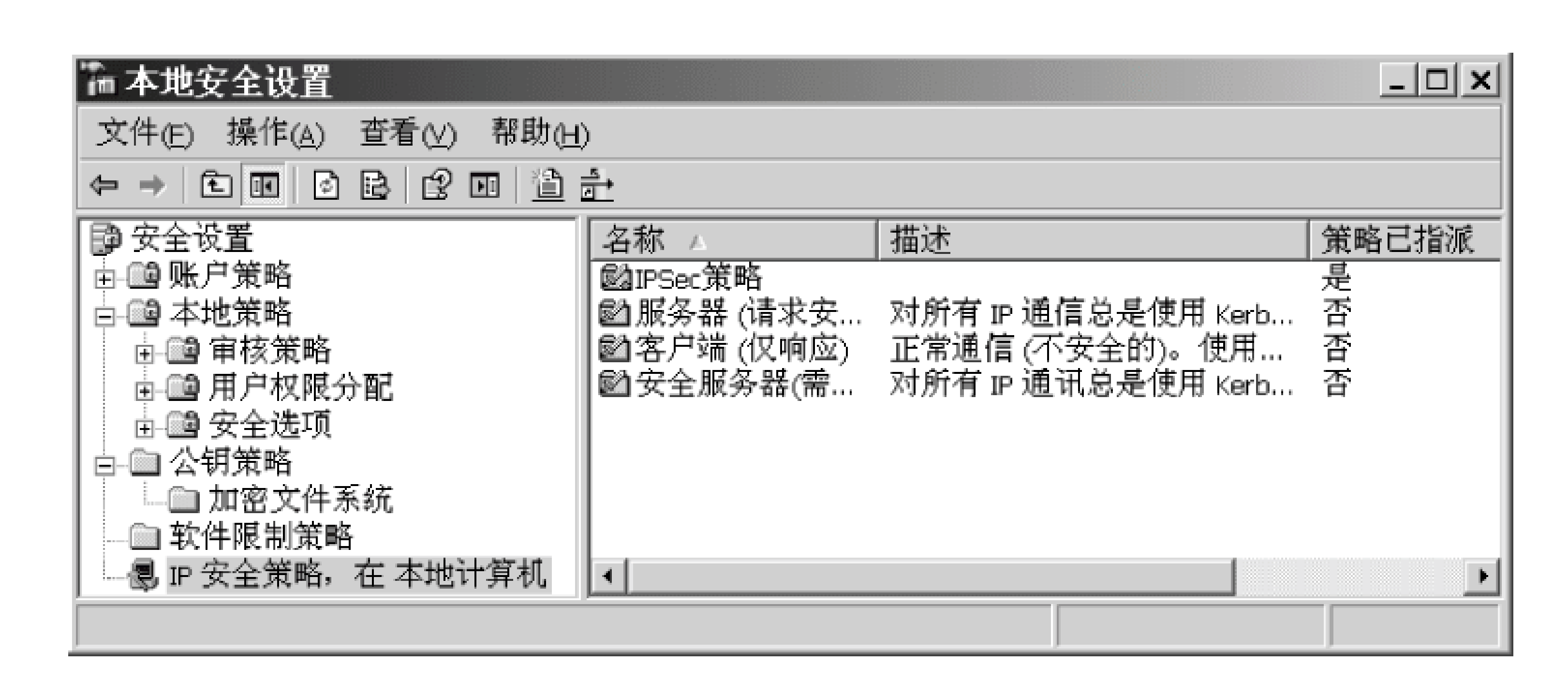


图 16-31 策略指派

16.4.3 任务 3：VPN 服务器的系统管理

1. 任务目标

主要描述对 VPN 自身进行的管理操作，如登录用户管理、系统时间配置、SSH 控制台管理、HA 设置管理、诊断工具管理以及配置信息备份和还原等。

2. 工作任务

(1) 连接及登录；

(2) VPN 服务器的系统管理。

3. 工作环境

两台预装 Windows Server 2003/XP 的主机，通过网络相连，其中一台有两张网卡。

4. 实施过程

(1) 连接及登录

① 单线接第 1 组蓝盾 VPN 的第一口，默认 IP 为 192.168.11.3，在 IE 输入 https://192.168.11.3；第 2 组蓝盾防火墙第一口，默认 IP 为 192.168.12.3；在 IE 输入 https://192.168.12.3；第 3 组蓝盾防火墙第一口，默认 IP 为 192.168.13.3；在 IE 输入 https://192.168.13.3；第 4 组蓝盾防火墙第一口，默认 IP 为 192.168.14.3；在 IE 输入 https://192.168.14.3；第 5 组蓝盾防火墙第一口，默认 IP 为 192.168.15.3；在 IE 输入 https://192.168.15.3；第 6 组蓝盾防火墙第一口，默认 IP 为 192.168.16.3；在 IE 输入 https://192.168.16.3；第 7 组蓝盾防火墙第一口，默认 IP 为 192.168.17.3；在 IE 输入 https://192.168.17.3；第 8 组蓝盾防火墙第一口，默认 IP 为 192.168.18.3；在 IE 输入 https://192.168.18. 3。统一用户密码为 admin/admin。

② 配置管理口 IP,单击“网络设置”→“接口设置”,然后对所需的网口进行配置,这里选择 LAN2 口。选择“编辑”,配置如图 16-32 所示。

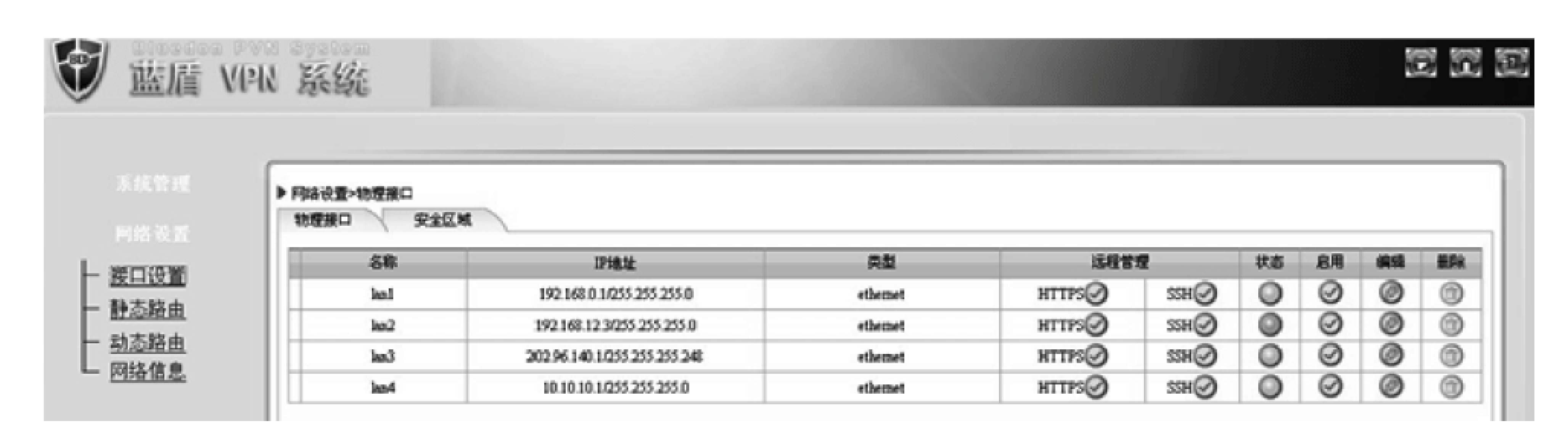


图 16-32　“接口设置”窗口

③ 单击“编辑”后,出现“物理接口”设置窗口,如图 16-33 所示。



图 16-33　“物理接口”设置窗口

④ 配置所需 IP 后,保存即可。

⑤ 配置静态路由,单击“网络设置”→“静态路由”,然后选择“添加”,再单击“保存”按钮,如图 16-34 所示。

(2) VPN 服务器的系统管理

系统管理包括系统信息、系统设置、登录管理、配置管理、SSH 控制台、HA 设置和诊断工具。

① 单击“系统管理”→“系统设置”按钮,进入“系统设置”页面,如图 16-35 所示。

系统设置用于配置 VPN 系统的基本信息,系统设置页面中的“语言”是指网页显示的语言;“主机名”是 VPN 服务器的主机名,要求最长 10 个字符;“域名”指 VPN 服务器的域名;“当前日期”设定为系统当前的日期;“当前时间”是系统当前的时间;“工作模式”是 VPN 服务器使用的工作模式。

② 单击“系统管理”→“系统配置”→“登录管理”按钮,进入“登录管理”页面,如图 16-36 所示。



图 16-34 “策略路由”设置窗口



图 16-35 “系统设置”窗口

▶ 系统管理>登录管理

系统设置　登录管理　配置管理　SSH控制台

用户名	有效时间	最后登录IP	最后登录时间	启用	编辑	删除
admin	36000s	100.100.100.25	2009-08-16 14:50			
audit	2500s					

图 16-36 “登录管理”窗口

“登录管理”用于管理用户，包括登录管理和权限管理。admin 可以管理所有用户，除了不能删除 admin 用户、修改 admin 用户权限外，可以拥有最大权限。另外，admin 可以查看用户的最后登录信息，其他用户只能查看自身的最后登录信息。

③ 单击“添加”按钮，进入用户添加界面，如图 16-37 所示。

图 16-37　添加用户

“基本信息”为必填项，包括用户名、密码、最大尝试次数与有效时间。“权限”为可选项，除了 admin 与 audit 用户不能修改外，其他的由客户自由配置。

④ 单击“系统管理”→“系统配置”→“配置管理”按钮，进入“配置管理”页面。此项用于保存当前最新配置信息，以及还原初始化。

⑤ 单击“系统管理”→“系统配置”→“SSH 控制台”按钮，进入“SSH 控制台”页面，这里可以不需要借用专门的 SSH 工具就能进入 VPN 后台配置管理。但进入“SSH 控制台”需要计算机安装 Java 软件包，不然无法操作。Java 软件包可在 http://www.java.com 下载。

⑥ 单击“系统管理”→“HA 设置”按钮，进入“HA 设置”页面，可以对 HA 群集进行设置，如图 16-38 所示。

图 16-38　HA 设置

在页面中选中“HA 启用”功能框即启动 HA 管理，HA 心跳保持 HA 状态信息的连续通信，确保群集工作正常，可以通过下拉框选择需要设置为心跳的接口。HA 心跳接口相互

通信群集会话信息、保持同步的群集配置与群集路由表并通报各个群集设备的状态信息。“VHID”是虚拟 IP 标识符,心跳内部通信所用。“密码”是共享的,在网络上不是明文传送,心跳内部通信所用。应该设置只监控与网络连接的接口,因为监控一个未连接的接口可能发生连接故障。“监控接口”必选,且可以选择多个,但不能与“心跳接口”相同。如果被监控的接口发生故障,例如,从网络断开或断开与群集的连接,会发生链接故障。链接故障使群集对该接口处理的数据包重新路由到群集中其他与网络连接的设备,因此该设备成为新的主设备。当断开的网线重新连接时,可以重新建立通过该接口的流量,接口将重新加入群集。

⑦ 单击“保存”按钮后,如果“HA 启用”功能框被启用,在页面会出现主机当前的运行状态:主服务器或是从服务器。当主机运行状态改变时,需要刷新页面,让其显示新的运行状态。当“HA 启用”功能框被禁用时,主机运行状态会被隐藏。

⑧ 单击“系统管理”→“诊断工具”按钮,进入诊断工具页面。常见的诊断工具有 ping、nslookup 和 traceroute。

16.5 常见问题解答

1. VPN 的“物理接口”设置界面中,各种图标的含义是什么?

答:图标 表示该功能启用,图标 表示该功能禁用;图标 表示该接口运行状态正常,图标 表示该接口运行状态异常;单击图标 可以对相应的网络接口进行编辑。

2. 如何保证 VPN 的安全性?

答:VPN 的安全性取决于使用的隧道协议和身份认证协议,以及应用于 VPN 连接的加密级别。在 TCP/IP 协议簇中,在数据链路层可以利用 L2F、PPTP、L2TP 协议实现 VPN 应用;在网络层可以利用 IPSec 协议实现 VPN 应用;在传输层利用 SSL 或 TLS 协议实现 VPN 应用。但是在 Windows Server 2003 的“路由和远程访问”中,仅支持 PPTP 和 L2TP 两种隧道协议来实现 VPN 服务。使用点对点隧道协议(PPTP)、点对点协议(PPP)身份认证协议和 Microsoft 点对点加密(MPPE)来加密 IP 通信。第二层隧道协议(L2TP)使用 PPP 用户身份认证协议和 Internet 协议安全性(IPSec)来加密 IP 通信,L2TP 将数据封装在 PPP 帧中传输。

16.6 过关练习

一、选择题

1. 关于虚拟专用网,下面正确的语句是(　　)。

A. 安全套接层协议(SSL)是在应用层和传输层之间增加的安全机制,可以用 SSL 在任何网络上建立虚拟专用网

B. 安全套接层协议(SSL)的缺点是进行服务器端对客服端的单向身份认证

C. 安全 IP 协议(IPSec)通过认证头(AH)提供无连接的数据完整性和数据源认证、数据加密性保护和抗重发攻击服务

D. 当 IPSec 处于传输模式时,报文不仅在主机到网关之间的通路上加密,而且在发送方和接收方之间的所有通路上都要加密

2. IPSec VPN 安全技术没有用到(　　)。

A. 隧道技术　B. 加密技术　C. 入侵检测技术　D. 身份认证技术

3. 实现 VPN 的关键技术主要有隧道技术、加解密技术、(　　)和身份认证技术。

A. 入侵检测技术　B. 病毒防治技术

C. 安全审计技术　D. 密钥管理技术

4. 如果需要在传输层实现 VPN,可选的协议是(　　)。

A. L2TP　B. PPTP　C. TLS　D. IPSec

二、填空题

1. IPSec 的密钥管理包括密钥的确定和分发,IPSec 支持________和________两种密钥管理方式。

2. IPSec 是 IETF 以 RFC 形式公布的一组安全协议集,它包括 AH 与 ESP 两个安全机制,其中________不支持保密服务。

3. 在 Windows Server 2003 的“路由和远程访问”中提供两种隧道协议来实现 VPN 服务:L2TP 和________。L2TP 协议将数据封装在________协议帧中传输。

三、简答题

1. 常见的 VPN 隧道协议有哪些?

2. VPN 技术的优势有哪些?

四、实操题

实现基于 Windows 的 VPN 通信。

参 考 文 献

1. 叶刚,陈文萍.黑客攻防实战入门与提高[M].北京:科学出版社,2011.
2. 黄传河,喻涛,王昭顺.网络安全防御技术实践教程[M].北京:清华大学出版社,2010.
3. 沈才梁.安全网络构建[M].北京:电子工业出版社,2010.
4. 迟恩宇,刘天飞,杨建毅,王东.网络安全与防护[M].北京:电子工业出版社,2009.
5. 刘晓辉.网络安全设计、配置与管理大全[M].北京:电子工业出版社,2009.
6. 石淑华,迟瑞楠.计算机网络安全技术[M].第2版.北京:人民邮电出版社,2008.
7. 孙连三.学以致用——黑客攻防实战入门[M].北京:人民邮电出版社,2009.
8. 陈小兵,张艺宝.黑客攻防实战案例解析[M].北京:电子工业出版社,2008.
9. 王达.网管员必读——网络安全[M].第2版.北京:电子工业出版社,2007.
10. 史晓红.网络安全完全技术宝典[M].北京:中国铁道出版社,2010.
11. 武新华,孙振辉.最新黑客攻防实战从入门到精通[M].北京:科学出版社,2011.
12. 武新华,翟长霖,安向东.黑客攻防从入门到精通[M].北京:科学出版社,2009.
13. 邓吉.黑客攻防实战入门[M].北京:电子工业出版社,2011.
14. 海吉.网络安全技术与解决方案[M].北京:人民邮电出版社,2010.
15. 九州书源.电脑黑客攻防[M].北京:清华大学出版社,2011.
16. 梵绅科技.新手学黑客攻防[M].北京:中国人民大学出版社,2009.
17. 石龙兴,周嘉鹏.信息安全综合实验指导书[M].广州:蓝盾信息安全技术股份有限公司,2011.
18. 全国计算机专业技术资格考试办公室.网络工程历年试题分析与解答[M].北京:清华大学出版社,2010.
19. 郭春柱.网络工程师软考辅导——3年真题透解与全真模拟[M].北京:机械工业出版社,2012.
20. 郭春柱.网络工程师考试案例梳理、真题透解与强化训练[M].北京:电子工业出版社,2009.
21. 软考新大纲研究组.网络工程师考试考眼分析与样卷解析[M].北京:机械工业出版社,2010.
22. 王文斌,王黎玲.计算机网络安全[M].北京:清华大学出版社,2010
23. 郝永清.堡垒主机搭建全攻略与流行黑客攻击技术深度分析[M].北京:科学出版社,2010.
24. 郝永清.黑客FTP攻击剖析与实用防御技术精解[M].北京:科学出版社,2010.